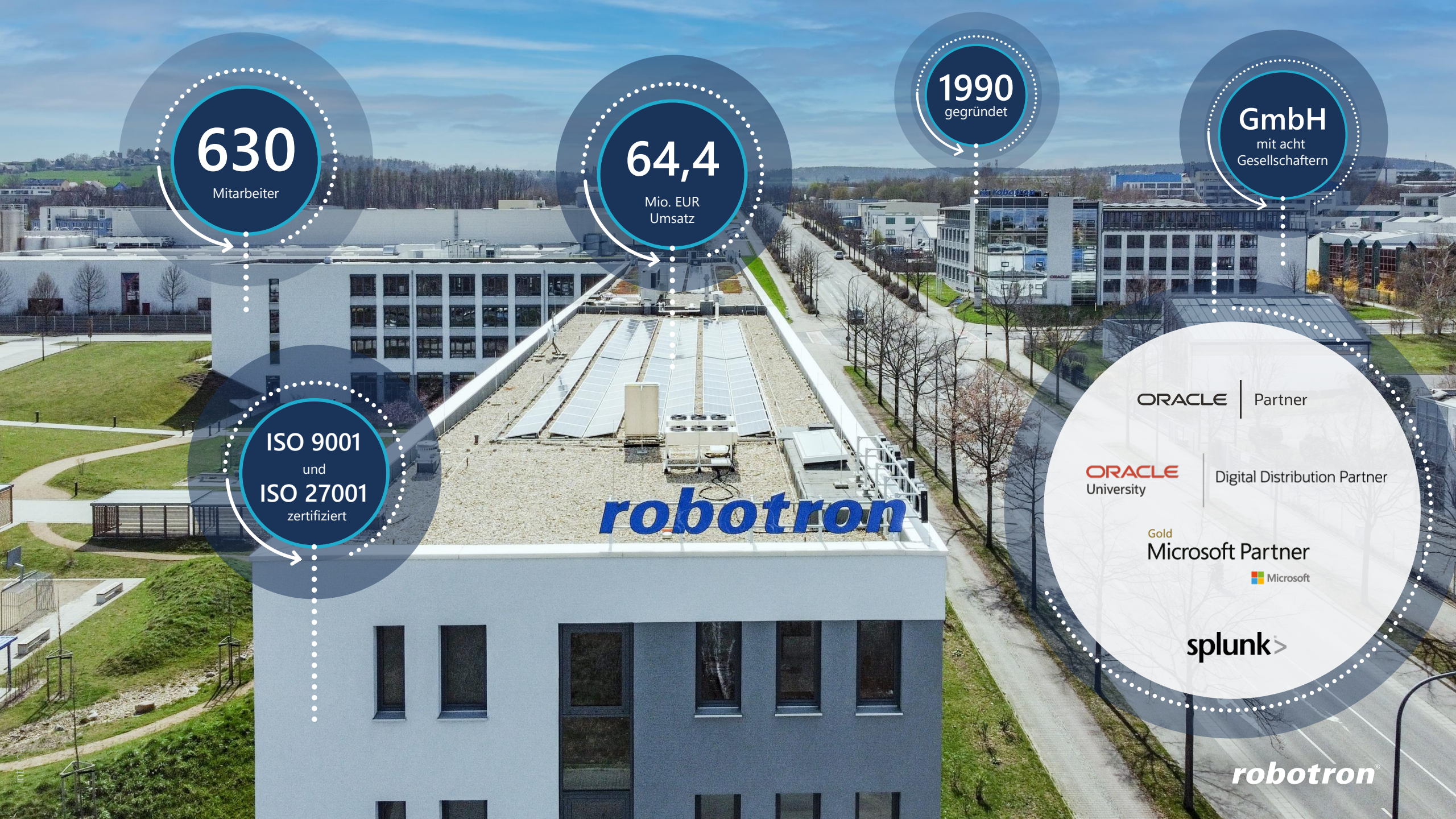
SOUGDay // Mittwoch // 17.04.2024 // 10:10 Uhr

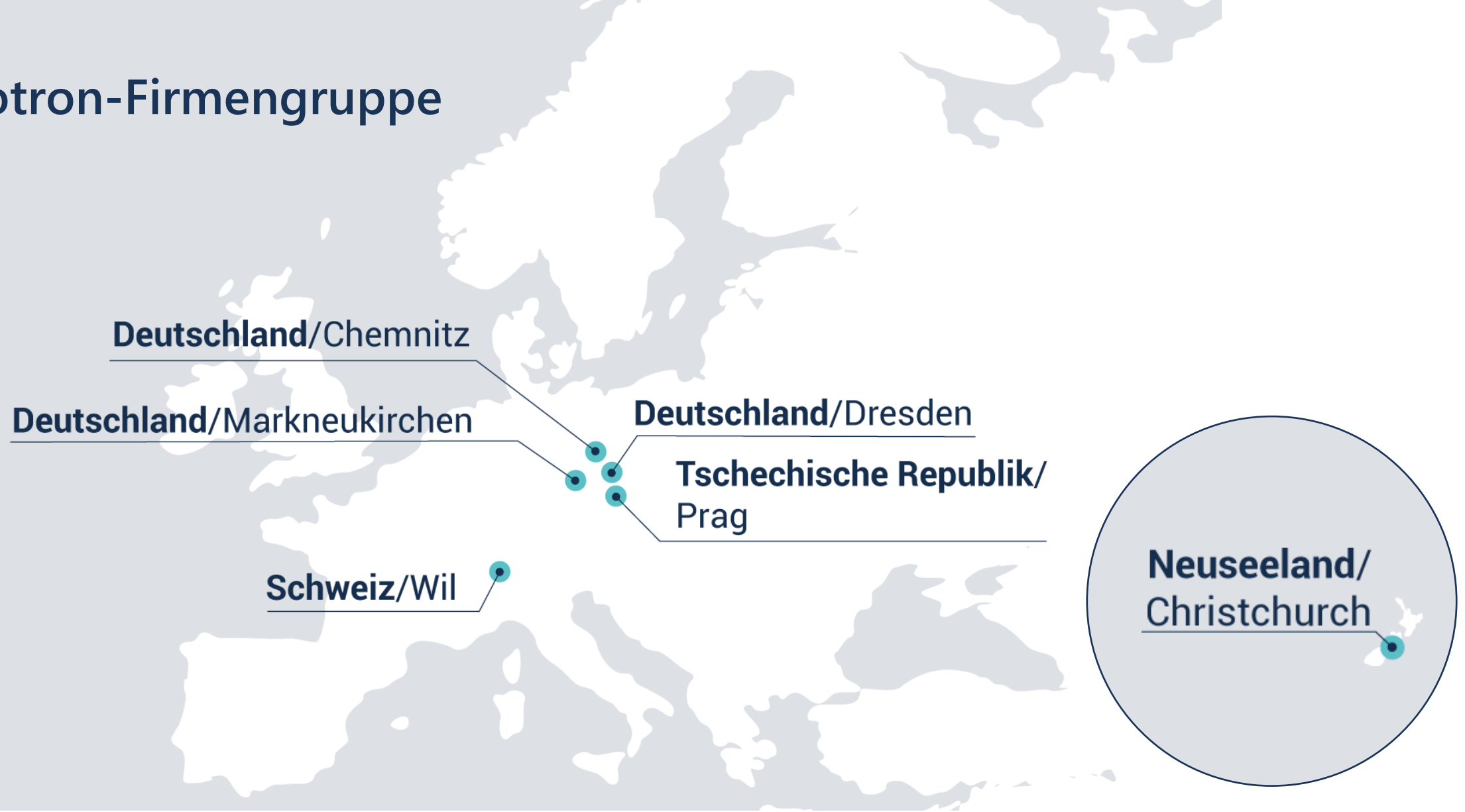
Security bei Multitenant-Architektur – Erfahrungen aus dem Alltag

Jörg Sobottka

robotron®


630
Mitarbeiter
64,4
Mio. EUR
Umsatz
1990
gegründet
GmbH
mit acht
Gesellschaftern
ISO 9001
und
ISO 27001
zertifiziert
ORACLE Partner
ORACLE University
Digital Distribution Partner
Gold
Microsoft Partner
Microsoft
splunk>
robotron
robotron

Robotron-Firmengruppe



robotron®

robotron® SCHWEIZ

robotron® CZECH REPUBLIC

robotron® NEW ZEALAND

SASKIA® Ein Unternehmen von robotron®

Vocus Ein Unternehmen von robotron®

MÄDER Computersysteme
Ein Unternehmen von robotron®

Oracle Datenbank Know-How (seit 1991)

Oracle Database Certified Professional (9i bis 12c)

Tuning und Hochverfügbarkeit, Systemarchitektur (>25 Jahre)

DB Software Design, DB Modellierung, Entwicklung (Forms, PL/SQL) (>20 Jahre)

Oracle Lizenzmanagement und unabh. Lizenzberatung (>20 Jahre)

Enterprise Manager Implementierung und Betrieb (> 20 Jahre)

Branchenkenntnisse: Energiewirtschaft, Touristik, Handel, Banken, Versicherungen und Öffentlicher Verkehr

Oracle ACE Pro

@JoergSobottka

https://a-different-view-by-js.blogspot.com

Robotron-BLOG

www.robotron.de/blog

Database and Engineered Systems

https://community.oracle.com

Agenda

Tja

Oha

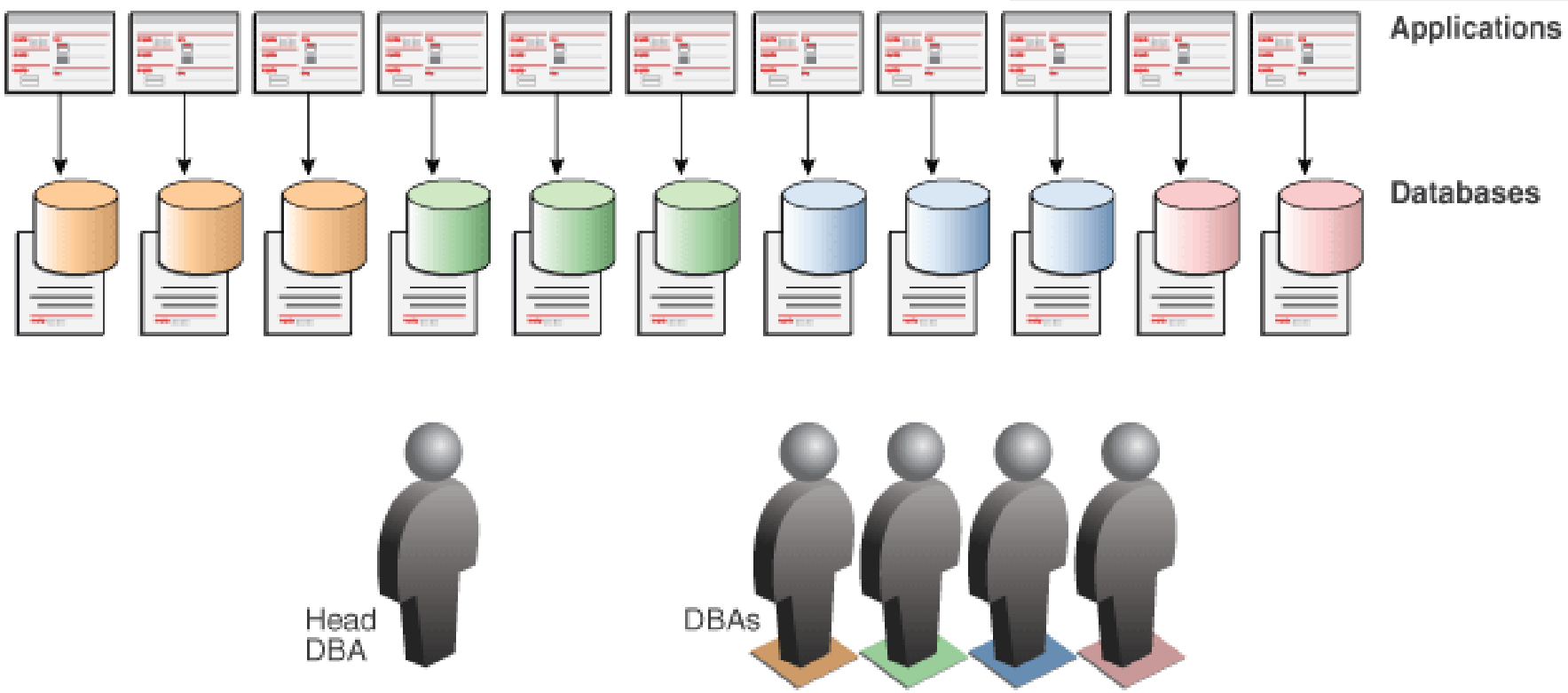
Aha

Oho

Tja!
- Damit musst Du leben.
- Ich hab’s Dir gesagt.
- Hättest Du mal auf mich gehört.
- Ganz schön verwirrend.

Tja!

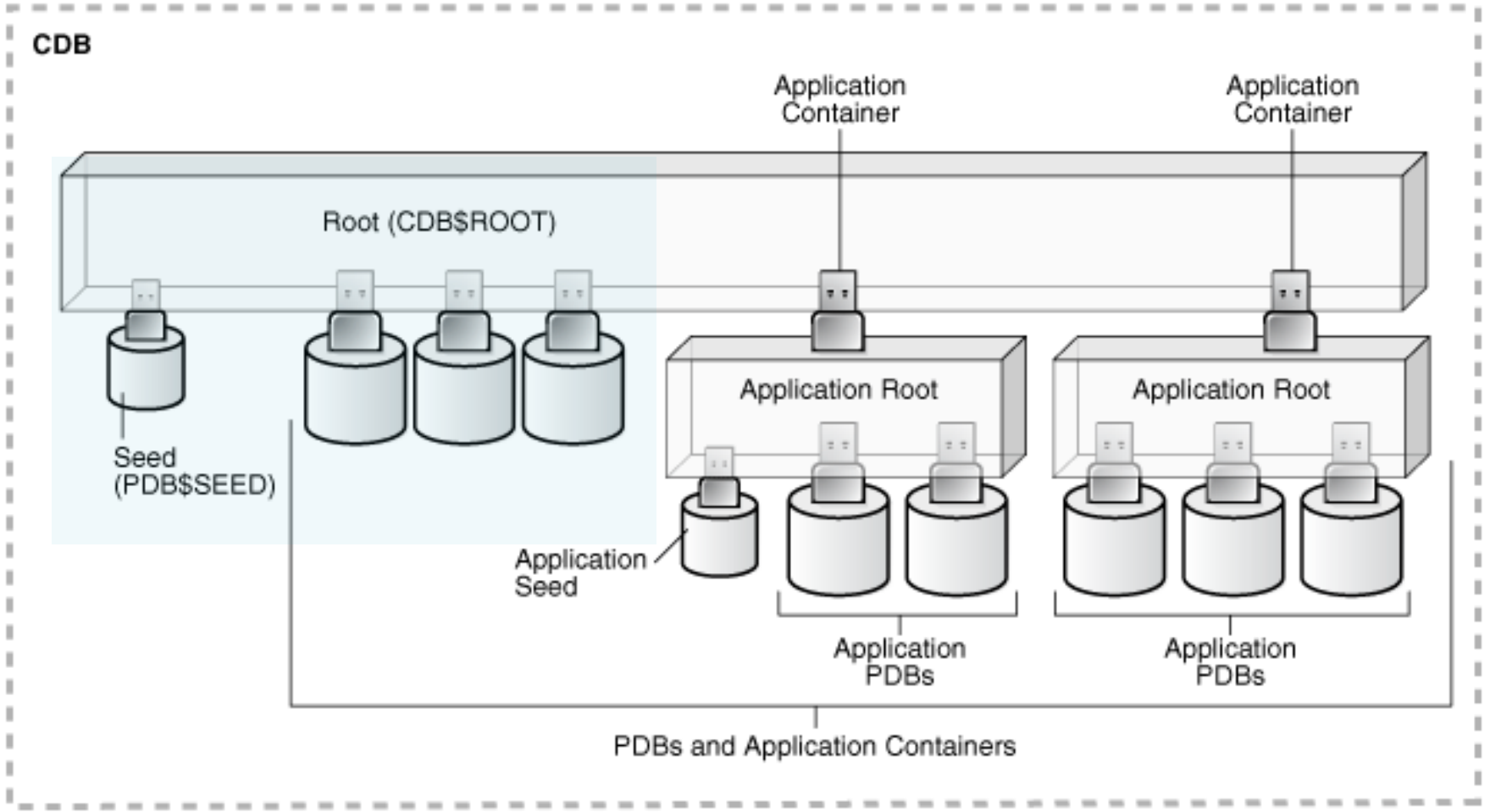
Klassische Architektur



Quelle: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html#GUID-DCE7F725-450E-4B58-ADBC-F51BED0637DE

Tja!

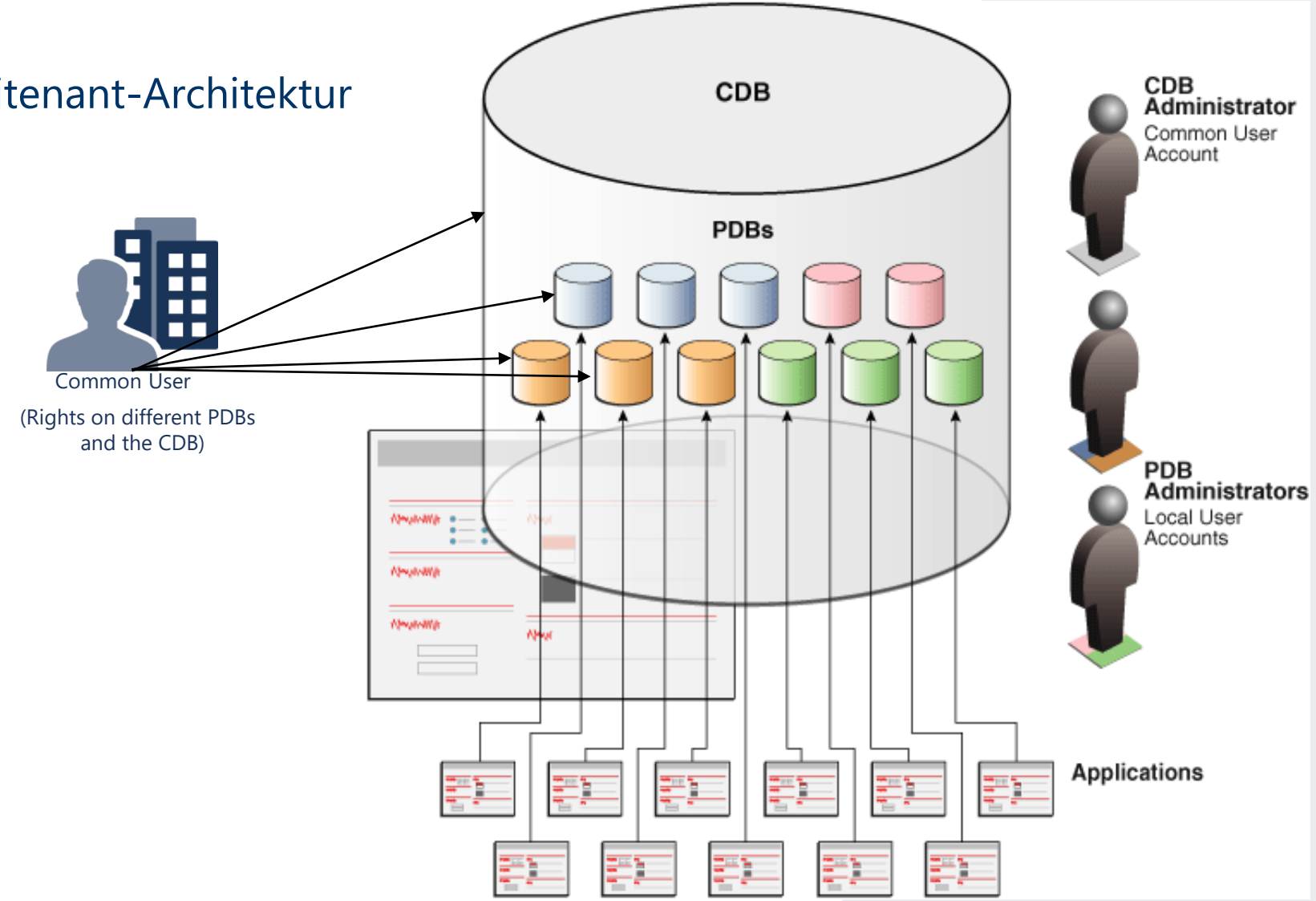
Multitenant-Architektur



Quelle: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html#GUID-DCE7F725-450E-4B58-ADBC-F51BED0637DE

Tja!

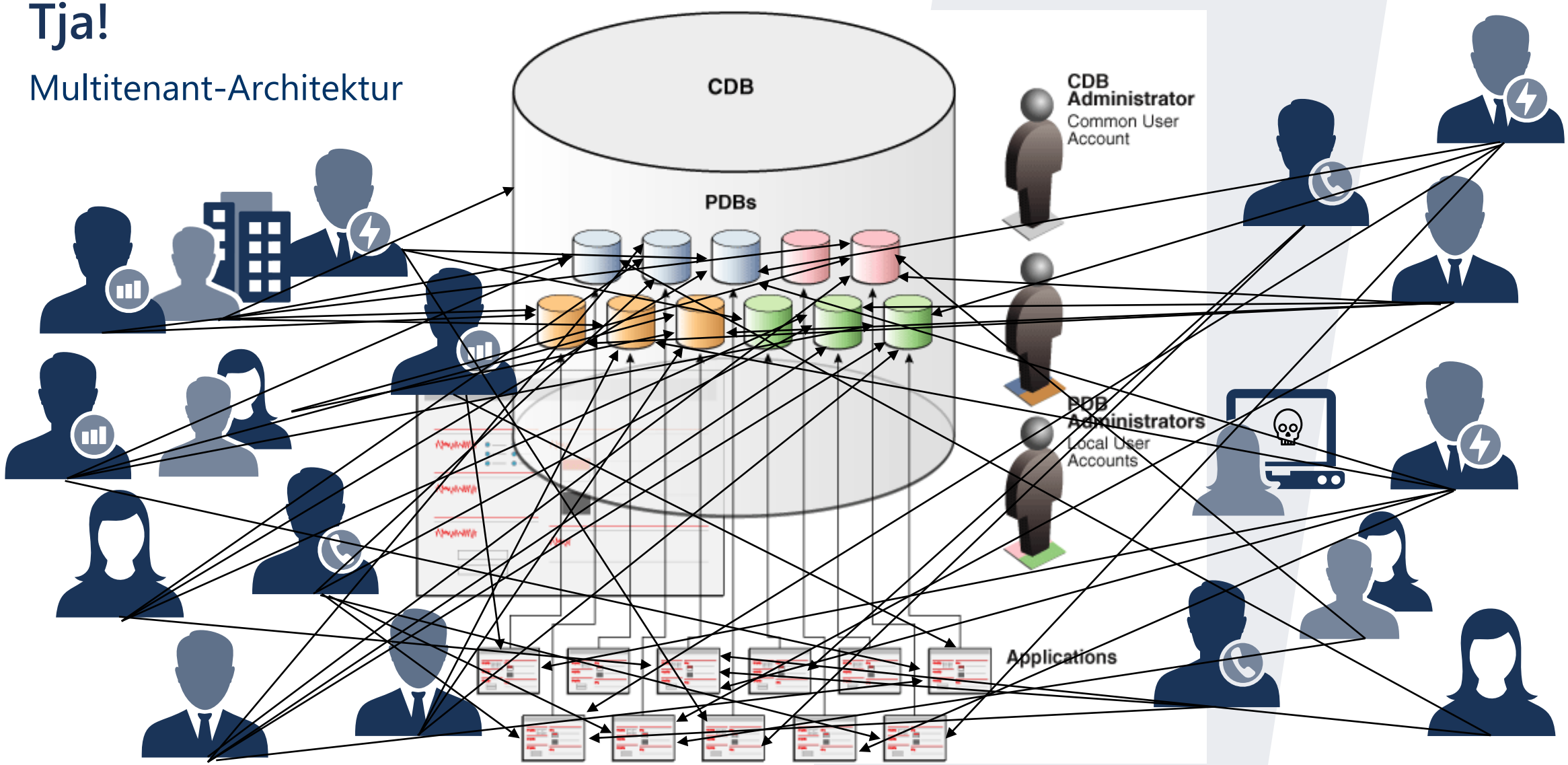
Multitenant-Architektur



Quelle: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html#GUID-DCE7F725-450E-4B58-ADBC-F51BED0637DE

Tja!

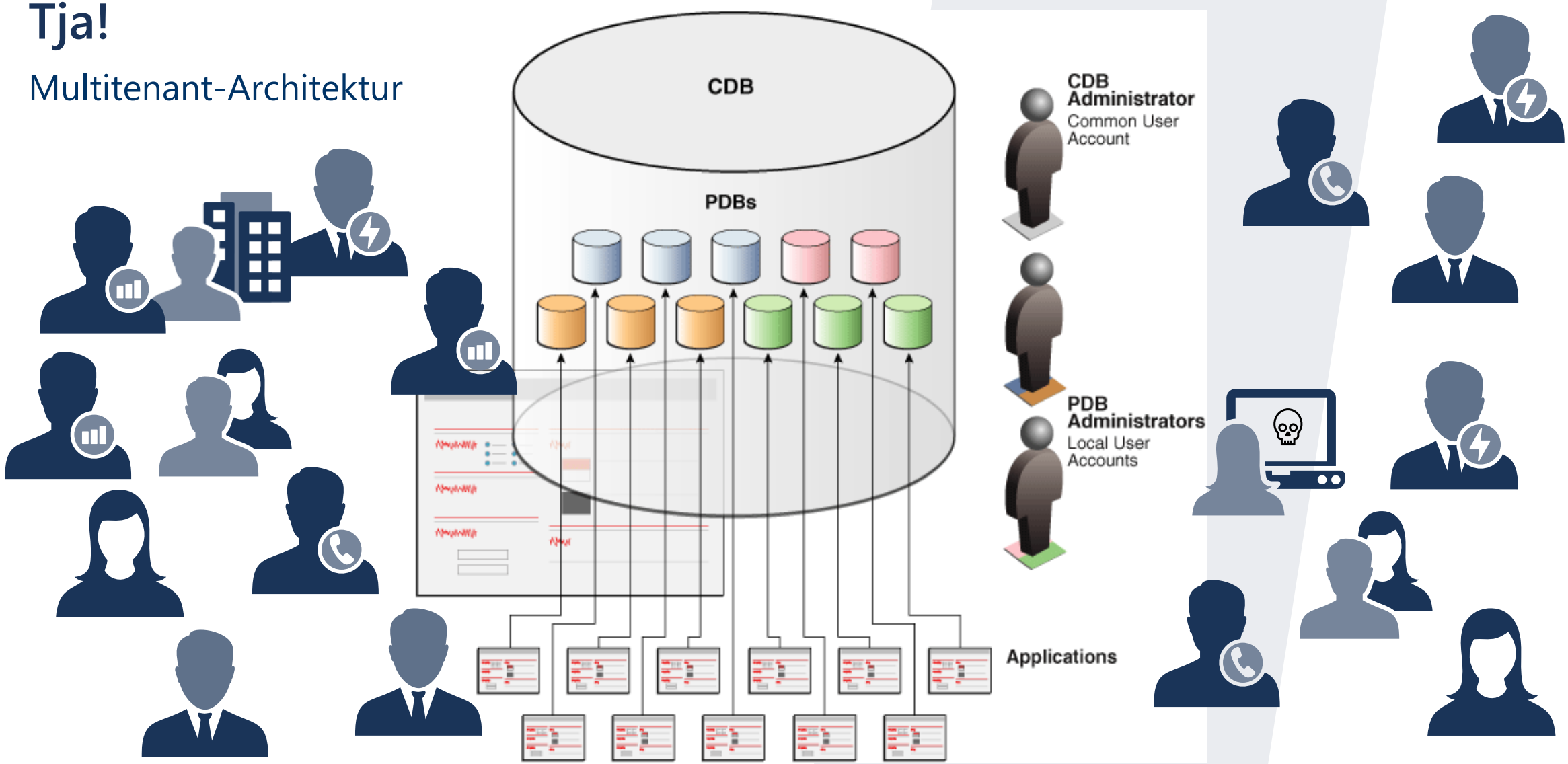
Multitenant-Architektur



Quelle: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html#GUID-22C7512B-024B-423B-8C29-73CB396A1D31

Tja!

Multitenant-Architektur



Quelle: https://docs.oracle.com/en/database/oracle/oracle-database/19/multi/introduction-to-the-multitenant-architecture.html#GUID-22C7512B-024B-423B-8C29-73CB396A1D31

Oha!
- Was?
- Warum das?
- (Norddeutsche Panikattacke)
- Oracle helps administrators(?).

Der PDB Administrator

Oha!

Oha! Der PDB Administrator

und seine Rechte

- Lokaler PDB User mit Rolle PDB_DBA
- Anlegen einer PDB von Seed:
  Create pluggable database <…>
  ADMIN USER <pdbadmin> identified by <password>;

```
SQL> create pluggable database pdb19_2 admin user pdb19_2_admin identified by oracle;

Pluggable database created.

SQL> select con_id,grantee,granted_role from cdb_role_privs where grantee='PDB19_2_ADMIN';

no rows selected
```

- PDB muss geöffnet werden!

Oha! Der PDB Administrator

und seine Rechte

```
  1* select con_id,grantee,granted_role from cdb_role_privs where grantee='PDB19_2_ADMIN'

  CON_ID GRANTEE         GRANTED_ROLE
-------- --------------- --------------
       4 PDB19_2_ADMIN   PDB_DBA
```

- sqlplus pdb19_2_admin/oracle@pdb19_2

```
SQL> select * from session_privs;

PRIVILEGE
----------------------------------------
```

Oha! Der PDB Administrator

und seine Rechte

```
  1* select con_id,grantee,granted_role from cdb_role_privs where grantee='PDB19_2_ADMIN'

  CON_ID GRANTEE         GRANTED_ROLE
-------- --------------- --------------
       4 PDB19_2_ADMIN   PDB_DBA
```

- sqlplus pdb19_2_admin/oracle@pdb19_2

```
SQL> select * from session_privs;

PRIVILEGE
----------------------------------------
CREATE PLUGGABLE DATABASE
CREATE SESSION
```

- Selbst «DBA» Rechte granten (an User oder Rolle)!

Oha! Der PDB Administrator

und seine Rechte

- « grant dba to pdb19_2_admin; »

```
SQL> select * from session_privs;

PRIVILEGE
----------------------------------------
DROP ANY ANALYTIC VIEW
ALTER ANY ANALYTIC VIEW
CREATE ANY ANALYTIC VIEW

...
ALTER SESSION
CREATE SESSION
AUDIT SYSTEM
ALTER SYSTEM

236 rows selected.
```

Oha! Der PDB Administrator

und seine Rechte

- « grant sysdba to pdb19_2_admin; »
- Einzelne Rechte mit Grant Option!
- Entspricht « SYSTEM » für PDBs
- Keine Rechte zur Anlage von Objekten in « SYS »
- Selects sind möglich (SYS-Objekte also im PDB Administrator anlegen)

```
SQL> shutdown immediate;
ORA-01031: insufficient privileges
```

```
SQL> create procedure sys.jso_test is
  2  begin
  3  null;
  4  end;
  5  /
create procedure sys.jso_test is
*
ERROR at line 1:
ORA-01031: insufficient privileges

SQL> select count(*) from sys.obj$;

  COUNT(*)
----------
     73695
```

Die Common User

Oha! Oha!

Oha! Common User

Gar nicht so einfach…

- Granten von Rechten (Bsp. Backup User):

```
SQL> create user c##backup_problem identified by oracle default tablespace users;

User created.

SQL> grant sysbackup to c##backup_problem;

Grant succeeded.
```

Oha! Common User

Gar nicht so einfach…

- Granten von Rechten (Bsp. Backup User):

```
Recovery Manager: Release 19.0.0.0.0 - Production on Tue Oct 11 11:00:10 2022
Version 19.16.0.0.0
RMAN> backup as compressed backupset database plus archivelog not backed up;


Starting backup at 11-OCT-22
current log archived
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=62 device type=DISK
skipping archived logs of thread 1 from sequence 37 to 43; already backed up
channel ORA_DISK_1: starting compressed archived log backup set
channel ORA_DISK_1: specifying archived log(s) in backup set
input archived log thread=1 sequence=44 RECID=29 STAMP=1117376670
input archived log thread=1 sequence=45 RECID=30 STAMP=1117736173
input archived log thread=1 sequence=46 RECID=31 STAMP=1117790516
                              ⋮
channel ORA_DISK_1: finished piece 1 at 11-OCT-22
piece handle=/u01/app/oracle/fast_recovery_area/ORCL19/backupset/2022_10_11/o1_mf_annnn_TAG20221011T111212_knbdvd3w_.bkp tag=TAG20221011T111212 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:01
Finished backup at 11-OCT-22

Starting Control File and SPFILE Autobackup at 11-OCT-22
piece handle=/u01/app/oracle/fast_recovery_area/ORCL19/autobackup/2022_10_11/o1_mf_s_1117797133_knbdvfh2_.bkp comment=NONE
Finished Control File and SPFILE Autobackup at 11-OCT-22
```

Oha! Common User

Gar nicht so einfach…

- Granten von Rechten (Bsp. Backup User): Datafile gelöscht

```
RMAN> repair failure;

Strategy: The repair includes complete media recovery with no data loss
Repair script: /u01/app/oracle/diag/rdbms/orcl19/orcl19/hm/reco_1892381711.hm

contents of repair script:
   # restore and recover datafile
   sql 'PDB19_1' 'alter database datafile 12 offline';
   restore ( datafile 12 );
   recover datafile 12;
   sql 'PDB19_1' 'alter database datafile 12 online';

Do you really want to execute the above repair (enter YES or NO)? yes
executing repair script

sql statement: alter database datafile 12 offline
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of repair command at 10/11/2022 11:47:15
RMAN-03015: error occurred in stored script Repair Script
RMAN-03009: failure of sql command on default channel at 10/11/2022 11:47:15
RMAN-11003: failure during parse/execution of SQL statement: alter session set container = PDB19_1
ORA-01031: insufficient privileges
```

Oha! Common User

Gar nicht so einfach…

- Granten von Rechten (Bsp. Backup User):

```
SQL> create user c##restore_test identified by oracle default tablespace users;

User created.

SQL> grant sysbackup to c##restore_test container=all;

Grant succeeded.
```

Oha! Common User

Gar nicht so einfach…

```
RMAN> repair failure;

Strategy: The repair includes complete media recovery with no data loss
Repair script: /u01/app/oracle/diag/rdbms/orcl19/orcl19/hm/reco_368685953.hm

contents of repair script:
   # restore and recover datafile
   sql 'PDB19_1' 'alter database datafile 12 offline';
   restore ( datafile 12 );
   recover datafile 12;
   sql 'PDB19_1' 'alter database datafile 12 online';

Do you really want to execute the above repair (enter YES or NO)? yes
executing repair script

sql statement: alter database datafile 12 offline

Starting restore at 11-OCT-22
using channel ORA_DISK_1

channel ORA_DISK_1: starting datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup set
channel ORA_DISK_1: restoring datafile 00012 to /u01/app/oracle/oradata/ORCL19/E5BBB3056DF6276DE0530F02000A97CF/datafile/o1_mf_users_knbgbmqw_.dbf
channel ORA_DISK_1: reading from backup piece /u01/app/oracle/fast_recovery_area/ORCL19/E5BBB3056DF6276DE0530F02000A97CF/backupset/2022_10_11/o1_mf_nnndf_TAG2022
1011T111016_knbds5oq_.bkp
channel ORA_DISK_1: piece handle=/u01/app/oracle/fast_recovery_area/ORCL19/E5BBB3056DF6276DE0530F02000A97CF/backupset/2022_10_11/o1_mf_nnndf_TAG20221011T111016_k
nbds5oq_.bkp tag=TAG20221011T111016
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
Finished restore at 11-OCT-22

Starting recover at 11-OCT-22
using channel ORA_DISK_1

starting media recovery
media recovery complete, elapsed time: 00:00:00

Finished recover at 11-OCT-22

sql statement: alter database datafile 12 online
repair failure complete
```

Oha! Common User

Gar nicht so einfach…

- Granten von Rechten (Bsp. Backup User):

```
Recovery Manager: Release 19.0.0.0.0 - Production on Tue Oct 11 12:22:08 2022
Version 19.16.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

RMAN> connect target "c##backup_problem/oracle@orcl19 as sysbackup"

connected to target database: ORCL19 (DBID=413522465)

RMAN> alter pluggable database pdb19_1 close;

using target database control file instead of recovery catalog
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of sql statement command at 10/11/2022 12:22:39
ORA-01031: insufficient privileges
```

Oha! Common User

Gar nicht so einfach…

- Entziehen von Rechten (Bsp. Backup User):

```
SQL> revoke sysbackup from c##backup_admin1 container=all;
RMAN> connect target 'c##backup_admin1/oraclebackup@orcl19 as sysbackup'

connected to target database: ORCL19 (DBID=413522465)

RMAN> backup datafile 1;

Starting backup at 08-NOV-22
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=85 device type=DISK
channel ORA_DISK_1: starting compressed full datafile backup set
channel ORA_DISK_1: specifying datafile(s) in backup set
input datafile file number=00001 name=/u01/app/oracle/oradata/ORCL19/datafile/o1_mf_system_kh21c3z7_.dbf
channel ORA_DISK_1: starting piece 1 at 08-NOV-22
channel ORA_DISK_1: finished piece 1 at 08-NOV-22
piece handle=/u01/app/oracle/fast_recovery_area/ORCL19/backupset/2022_11_08/o1_mf_nnndf_TAG20221108T210957_kpofwol8_.bkp tag=TAG20221108T21095
7 comment=NONE
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:35
Finished backup at 08-NOV-22

Starting Control File and SPFILE Autobackup at 08-NOV-22
piece handle=/u01/app/oracle/fast_recovery_area/ORCL19/autobackup/2022_11_08/o1_mf_s_1120252232_kpofxrsz_.bkp comment=NONE
Finished Control File and SPFILE Autobackup at 08-NOV-22
```

Oha! Common User

Gar nicht so einfach…

- Entziehen von Rechten (Bsp. Backup User):

```
SQL> revoke sysbackup from c##backup_admin1;

Revoke succeeded.

RMAN> connect target 'c##backup_admin1/oraclebackup@orcl19 as sysbackup'

RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
ORA-01017: invalid username/password; logon denied
```

Oha! Common User

Gar nicht so einfach…

- Entziehen von Rechten (Bsp. Backup User):

```
RMAN> connect target 'c##backup_admin1/oraclebackup@pdb19_1 as sysbackup'

connected to target database: ORCL19:PDB19_1 (DBID=3155075316)

SQL> revoke sysbackup from c##backup_admin1 container=pdb19_1;
revoke sysbackup from c##backup admin1 container=pdb19 1
RMAN> connect target 'c##backup_admin1/oraclebackup@pdb19_1 as sysbackup'

RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
ORA-01017: invalid username/password; logon denied
Session altered.

SQL> revoke sysbackup from c##backup_admin1;

Revoke succeeded.
```

Oha! Common User

Gar nicht so einfach…

- Rechte des Benutzers VOR Revoke:

```
SQL> select username, sysbackup, con_id from v$pwfile_users
  2  where username='C##BACKUP_ADMIN1';

USERNAME                                 SYSBACKUP      CON_ID
---------------------------------------- ---------- ----------
C##BACKUP_ADMIN1                         TRUE                0
C##BACKUP_ADMIN1                         TRUE                1
C##BACKUP_ADMIN1                         TRUE                3
```

```
SQL> select con_id, name from v$containers;

    CON_ID NAME
---------- ------------------------------
---------- ------------------------------
         1 CDB$ROOT
         2 PDB$SEED
         3 PDB19_1
```

```
SQL> revoke sysbackup from c##backup_admin1 container=all;

Revoke succeeded.

SQL> select username, sysbackup, con_id from v$pwfile_users where
username='C##BACKUP_ADMIN1';

USERNAME                                 SYSBACKUP      CON_ID
---------------------------------------- ---------- ----------
C##BACKUP_ADMIN1                         TRUE                1
C##BACKUP_ADMIN1                         TRUE                3
```

Oha! Common User

Gar nicht so einfach…

- Rechte des Benutzers:

```
SQL> select username, sysbackup, con_id from v$pwfile_users
  2  where username='C##BACKUP_ADMIN1';

USERNAME                                 SYSBACKUP      CON_ID
---------------------------------------- ---------- ----------
C##BACKUP_ADMIN1                         TRUE                0
C##BACKUP_ADMIN1                         TRUE                1
C##BACKUP_ADMIN1                         TRUE                3
```

```
SQL> select con_id, name from v$containers;

    CON_ID NAME
---------- ------------------------------
---------- ------------------------------
         1 CDB$ROOT
         2 PDB$SEED
         3 PDB19_1
```

```
SQL> revoke sysbackup from c##backup_admin1;

Revoke succeeded.

SQL> select username, sysbackup, con_id from v$pwfile_users where
username='C##BACKUP_ADMIN1';

USERNAME                                 SYSBACKUP      CON_ID
---------------------------------------- ---------- ----------
C##BACKUP_ADMIN1                         TRUE                3
```

Oha! Common User

Gar nicht so einfach…

- Rechte des Benutzers:

```
SQL> select userna
  2  where usernam

USERNAME
--------------------
C##BACKUP_ADMIN1
C##BACKUP_ADMIN1
C##BACKUP_ADMIN1

SQL> select con_id

    CON_ID NAME
---------- -------
---------- -------
         1 CDB$ROO
         2 PDB$SEE
         3 PDB19_1
```

```
SQL> alter session set container=pdb19_1;

Session altered.

SQL> revoke sysbackup from c##backup_admin1;

Revoke succeeded.

SQL> alter session set container=cdb$root;

Session altered.

SQL> col username format a40
SQL> col sysbackup format a10
SQL> select username, sysbackup, con_id from v$pwfile_users
  2   where username='C##BACKUP_ADMIN1';

no rows selected
```

```
kup_admin1;

con_id from v$pwfile_users where

                                         SYSBACKUP      CON_ID
---------- ------- ---------- ----------
                                         ---------- ----------
                                         C##BACKUP_ADMIN1
                                         TRUE                3
```

Aha!
- Okay.
- So ist das.
- Na denn.
- Du kannst mich mal.

robotron®

Aha! Common User

Gar nicht so einfach…

- Merke:
  - Common User und Rechte granten/revoken ist nicht einfach
  - „SysBackup“ ist einfach – Problem: Grants auf Objekte, Rollen in verschiedenen PDBs und in der CDB.
  - Revoke kann kompliziert sein
    Workaround: Common User droppen, neu anlegen
  - User mit zentralen, vorgegebenen/eigenen Rollen anlegen (z.B. „CDB DBA“, „Connect“) statt einzeln Rechte zu granten
    (https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-privilege-and-role-authorization.html#GUID-A5B26A03-32CF-4F5D-A6BE-F2452AD8CB8A)

Aha!

Transport Layer Security (TLS) in SE 2 und EE

- Eigene Wallets pro PDB
- sqlnet.ora – CDB Lokation angeben!
  (SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/u01/app/wallets/MYCDB)))
- CDB Wallet in /u01/app/wallets/MYCDB/TLS
- Unterverzeichnis GUID der PDB anlegen und PDB Wallet dort erstellen/ablegen
  select name, guid from v$containers;

NAME	GUID
CDB$ROOT	52448234712340B69F274BCC790ECFE0
PDB$SEED	1643707480094E118AE90512A5975CE6
SPATEST	CC8927A462D6444CA3CBF334C7AE7A02

- SPATEST Wallet in /u01/app/wallets/MYCDB/CC8927A462D6444CA3CBF334C7AE7A02/TLS
- alter system set wallet_root='/u01/app/wallets/MYCDB ' scope=spfile sid='*';
- Nicht vergessen: Für Client-Verbindungen „orapki wallet export“ des Zertifikats der PDB und ggfs. CDB getrennt erforderlich

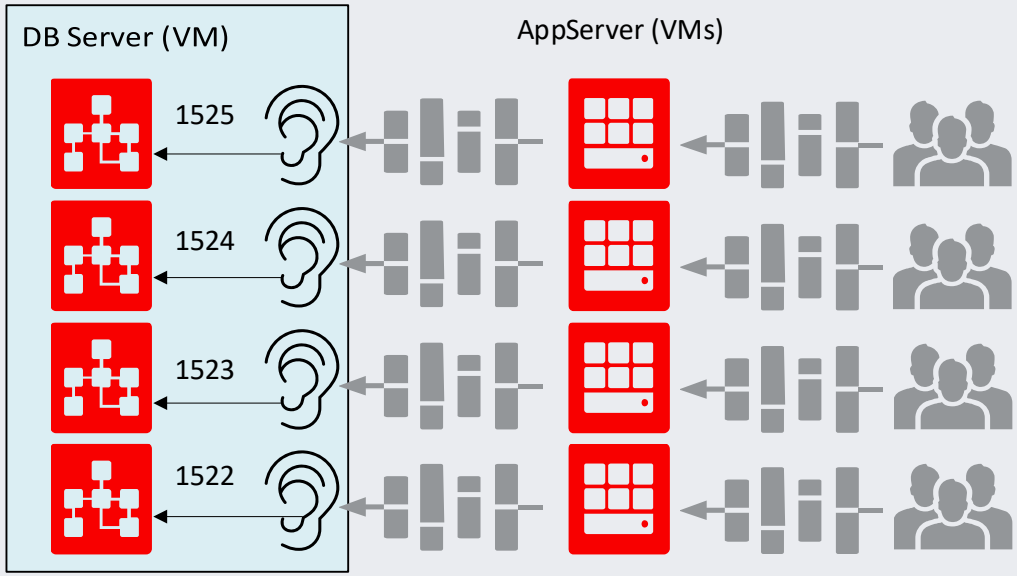
Aha!

Mehr Connection Security

Ist-Zustand

- Unterwegs in der Cloud (Windows VM als DB Server + diverse AppServer)
- Betreibt X Datenbanken für Endkunden
- Ein bis Zwei PDBs pro DB
- Teilweise Y DBs auf gleichem Server mit Y Listenern (und eigenem DB Home)
- Jede (P)DB hat eigenen AppServer (eigene VM)
- Anzahl Firewallregeln
- Patching, neuer Kunde, Testsysteme
- Security

Schema



Aha!

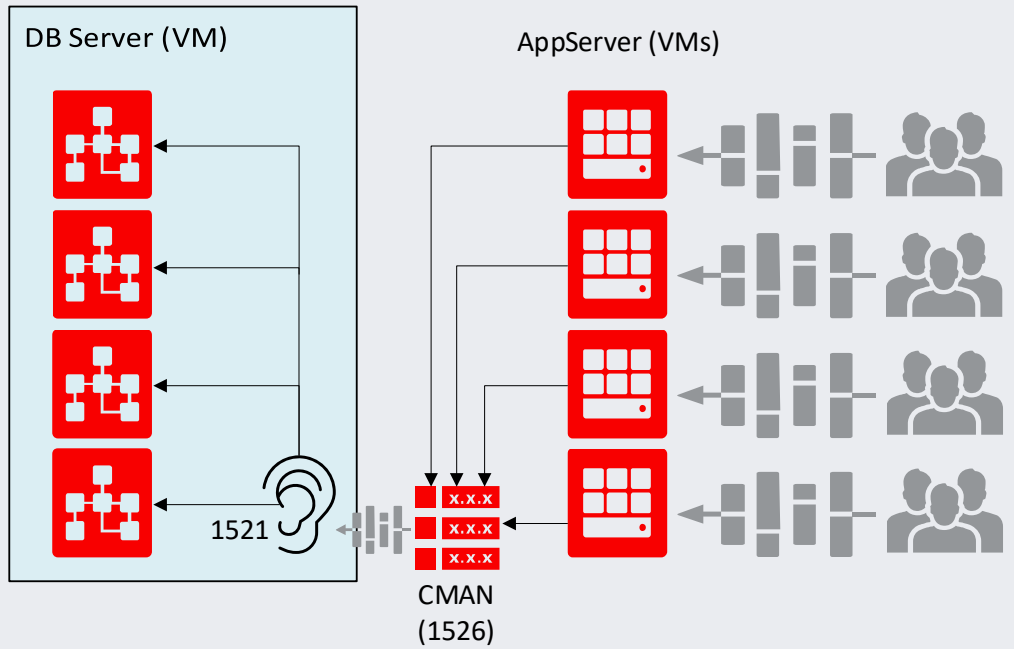
Mehr Connection Security

Soll-Zustand Enterprise Edition

- Ein Listener auf dem DB Server
- Ein Oracle Home auf dem DB Server
- Keine komplizierten Firewall-Regeln zwischen AppServer und DBServer
- Connection Manager mit Rule List (Port 1526)

```
(RULE_LIST=
  (RULE=
    (SRC=host/*/Subnet 192.0.2.32/27)
    (DST=host)
    (SRV=service_name)
    (ACT={accept|reject|drop})
    (ACTION_LIST=AUT={on|off}
  )
  (RULE= ...))
```

Schema



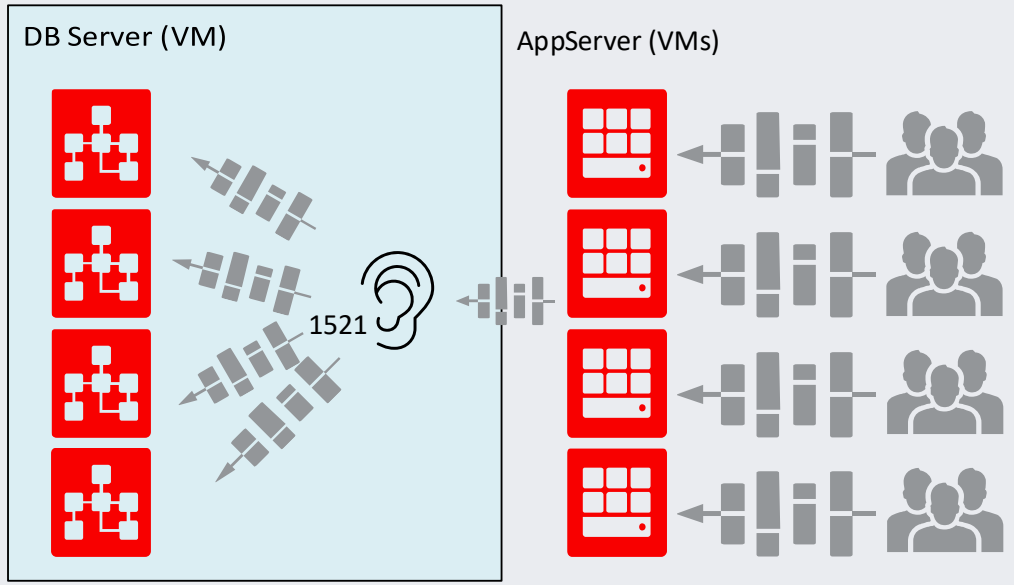
Aha!

Mehr Connection Security

Soll-Zustand Standard Edition 2

- Ein Listener auf dem DB Server
- Ein Oracle Home auf dem DB Server
- Keine komplizierten Firewall-Regeln zwischen AppServer und DBServer
- Firewall für PDB Service über Listener
- Definiert in der Datenbank
- dbsfwuser.DBMS_SFW_ACL_ADMIN.ip_add_ace

Schema



Aha!

Mehr Connection Security

Oho!
- Das hätte ich nicht gedacht.
- Ich werd verrückt.
- Mann, Mann, Mann.
- Unglaublich.

robotron®

Oho!

Auditing

- Sehr hilfreich, z.B. auf Rolle „DBA“!
- Container Clause nicht vergessen!
  CREATE AUDIT POLICY policy_name action1 [,action2] [CONTAINER = {CURRENT | ALL}];
- Common Audit Policies haben nur Zugriff auf Common Objekte
- Lokale (CDB$ROOT oder PDB) Audit Policies haben Zugriff auf Common Objekte und lokale Objekte
- Abfragen mit „CON_ID“ oder „DBID“ in CDB_UNIFIED_AUDIT_TRAIL

Lockdown Profile

- Erlauben/verhindern „Alter System“ oder Feature Usage
- Profile werden kaum verwendet (weder vorhandene „Private_DBaaS, Public_DBaaS, SaaS“ noch eigene)
- „Zu kompliziert“ / „Zu wenig spezifisch“ / „da fehlt“

Sicher ist, dass nichts sicher ist. Selbst das nicht.

Joachim Ringelnatz

Konzepte erstellen!
Konzepte umsetzen!
Auditieren/Überwachen!

Jörg Sobottka

Jörg Sobottka

Senior-Berater

joerg.sobottka@robotron.ch
071 225 78 04

intern

robotron®