CARAJANDB

Oracle Security Basics

Johannes Ahrends

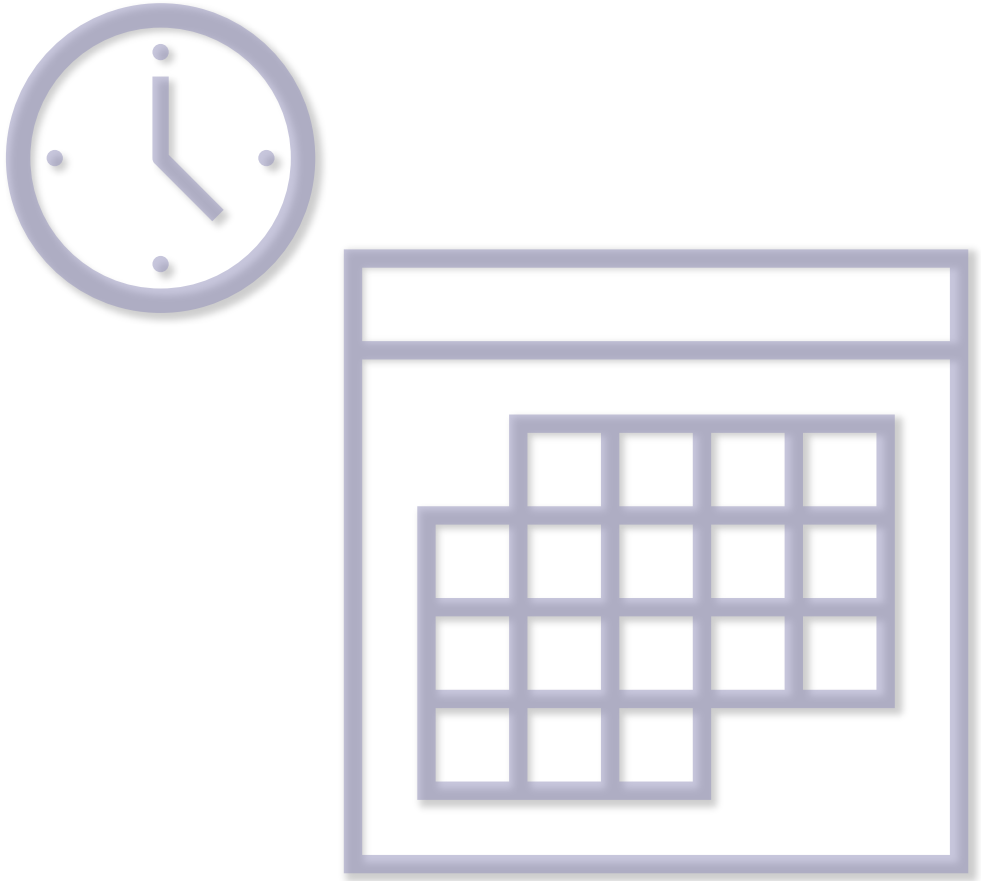
… über mich

- Oracle Spezialist seit 1992
  - 1992: Presales bei Oracle in Düsseldorf
  - 1999: Projektleiter bei Herrmann & Lenz Services GmbH
  - 2005: Technischer Direktor ADM Presales bei Quest Software GmbH
  - 2011: Geschäftsführer CarajanDB GmbH
- 2011 → Ernennung zum Oracle ACE
- DOAG-Themenverantwortlicher Datenbankadministration, Standard Edition
- DOAG-Botschafter
- Autor der Bücher
  - Oracle9i für den DBA, Oracle10g für den DBA, Oracle 11g Release 2 für den DBA
- Hobbies:
  - Drachen steigen lassen (Kiting) draußen wie drinnen (Indoorkiting)
  - Motorradfahren (nur draußen)
  - Singen (überall)

Agenda

Der DBA

Accounts



CARAJANDB

Wer akzeptiert standardmäßig alle Vorwürfe?

Der D.B.A.

Default Blame Acceptor

Server Logon Linux

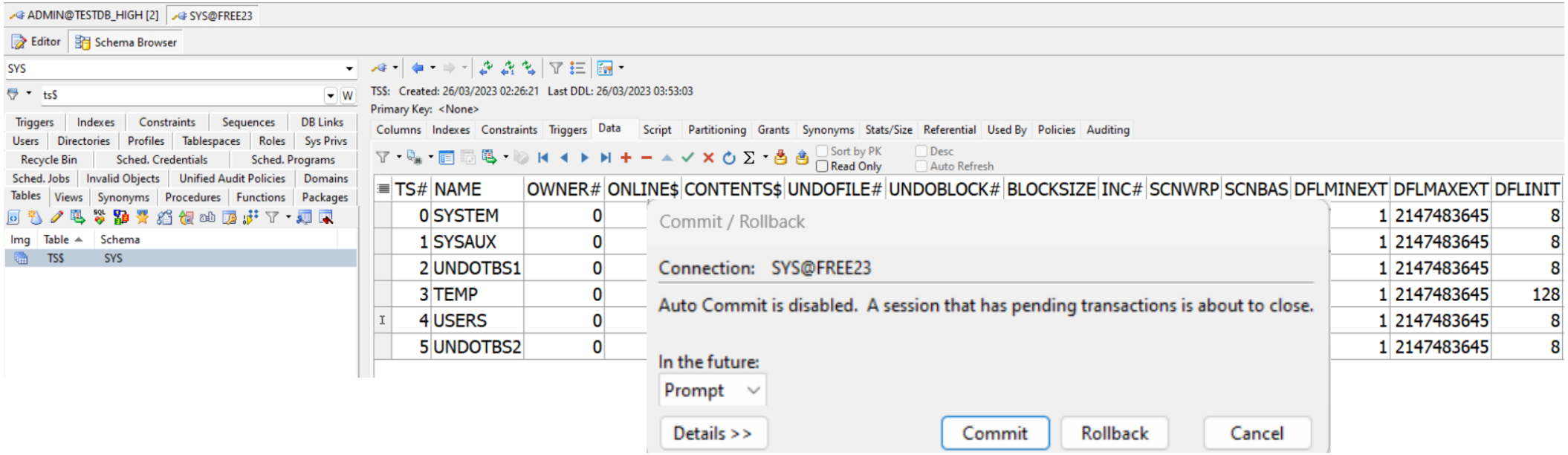
- Anmeldung als „**`root`**“ und **`su`** auf „**`oracle`**“➔ der DBA ist an allem schuld!
- Besser:
  - Anmeldung über persönlichen Account
  - **`sudo su - oracle`** oder **`grid`**
  - **`sudo`** von root-Befehlen
  - Protokollieren der Session (z.B. Mobaxterm oder putty Log

- Frage: Warum musste ich zu diesem Zeitpunkt auf diesen Server?
  - Ticket hilft

SYS ACCOUNT

User SYS

- Besitzer der Datenbank



… IDENTIFIED BY VALUES

- Anlegen eines Benutzers, ohne das Passwort zu kennen
  - Z.B. bei Data Pump Export / Import
  - Ungültiges Passwort (`IDENTIFIED BY VALUES 'GEHEIM'`)
- Spalte `SPARE4` in der Tabelle `USER$`

```
SELECT name, spare4 FROM user$ WHERE name = 'SYSTEM'

NAME       SPARE4
---------- ----------------------------------------------------------------
SYSTEM     S:029D81DEA529106A767BDF686778897B1185B2DA5CD0D1C285D5610076DE;T:67168
           12B4964575A9F6E83F19E5A3FC7FBDB6FEBC7A0D0D574B64386359FFE6ED39C4F2E7BA
           140D07BF5B6EF1CE40593986122EE2AED5E7EA090EC60939C0A98701CF21D69DE5C3FA
           2B2E4D1DFD865B6
```

- S: Oracle 11g SHA-1 Verschlüsselung
- T: Oracle 12c SHA-512 Verschlüsselung

Vorschlag

- Nur Persönliche User als DBAs definieren
  - Mit der selbst definierten Rollen
- Technischer User für Anwendungen
  - ggf. mit Wallet Passwort
- Trennung von User und Schema
  - Dem Schema gehören die Objekte (nur DDL)
    - Schema gesperrt
  - Der User hat Zugriff auf die Objekte (nur DML)
- Common User immer mit C## Prefix

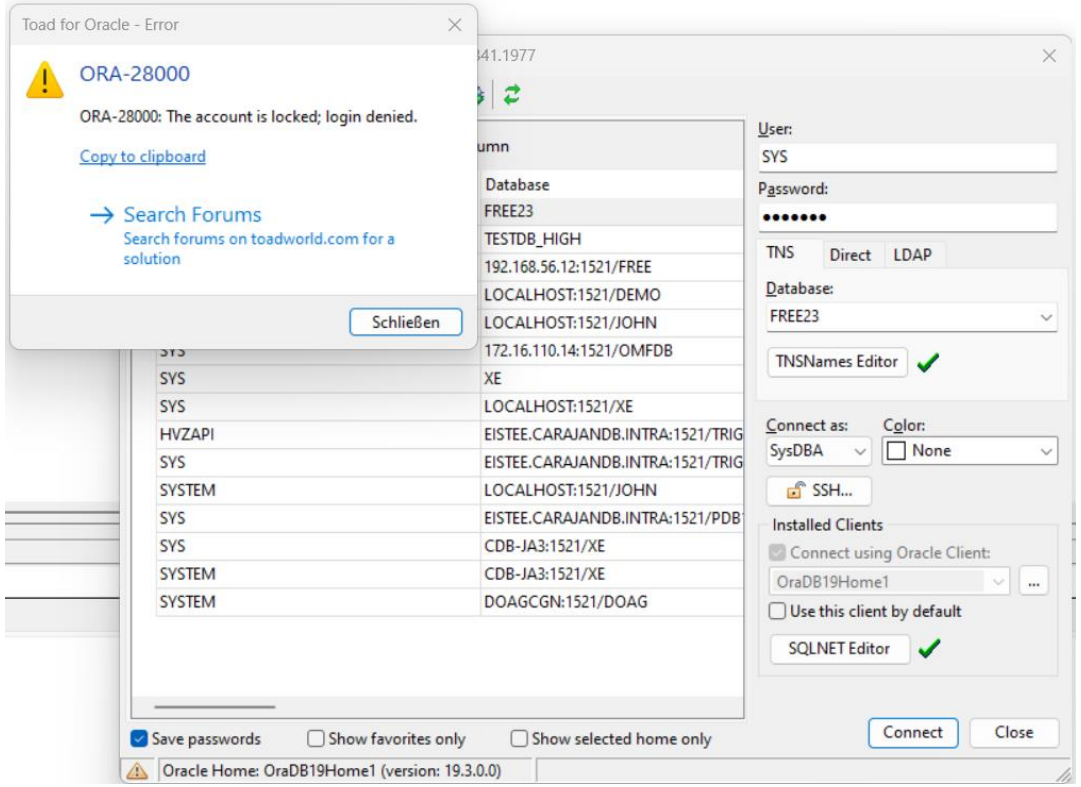
orapwd

```
format - use format=12 for longer identifiers,
             SHA2 Verifiers etc.
             use format=12.2 for 12.2 features like enforcing user
             profile (password limits and password complexity) and
             account status for administrative users.
             If not specified, format=12.2 is default (optional),
```

```
% orapwd file=$ORACLE_HOME/dbs/orapwFREE sys=y format=12.2 force=y

Enter password for SYS:
OPW-00029: Password complexity failed for SYS user : Password must contain at least
1 special character.

% orapwd file=$ORACLE_HOME/dbs/orapwFREE sys=y format=12.2 force=y

Enter password for SYS:
```

Lock User SYS

```
SQL> ALTER USER sys ACCOUNT LOCK;
User altered.
```



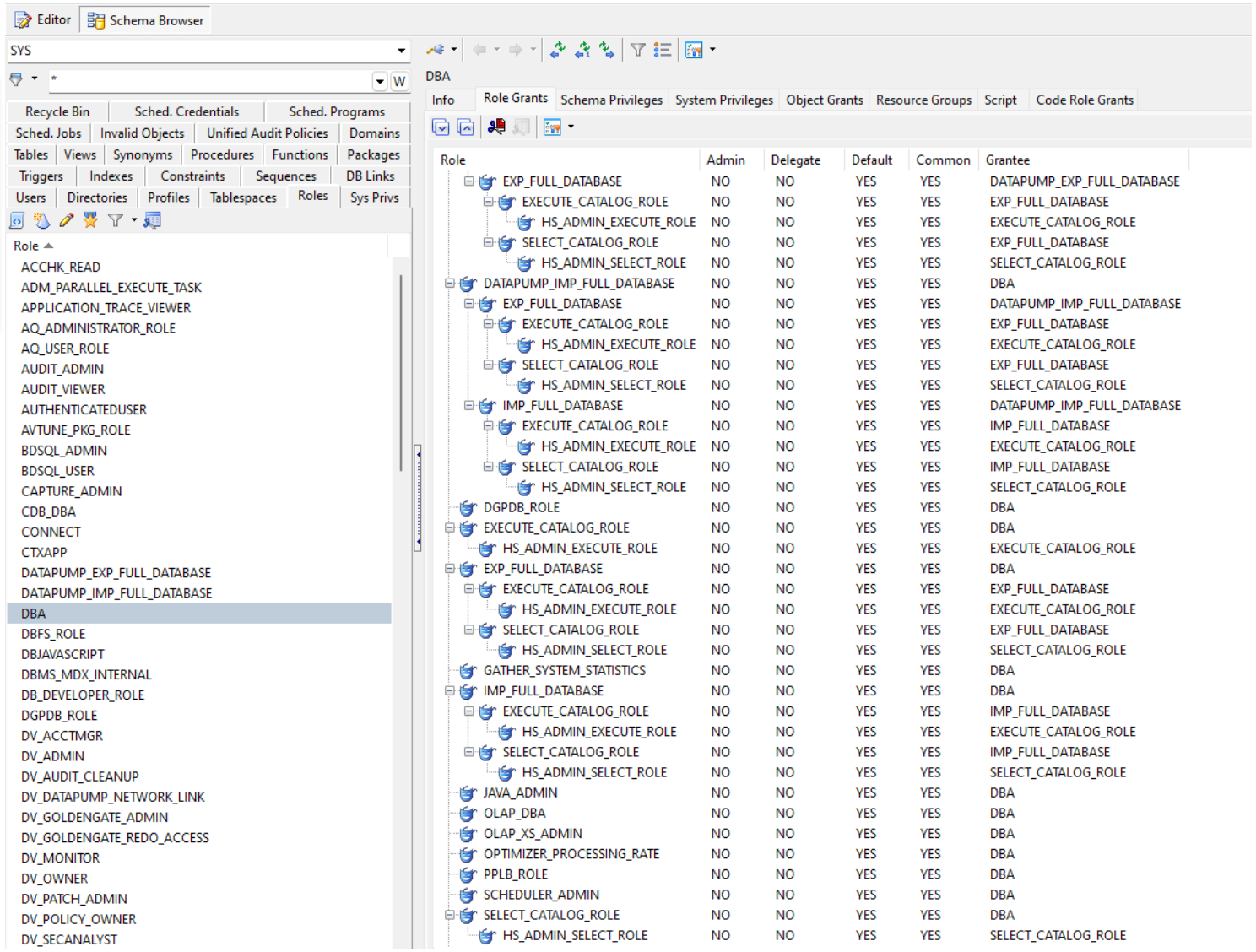
Frage

Wie viele Rechte und Rollen hat die DBA Rolle?

DBA Rolle

```
• SELECT count(*)
FROM   sys.dba_role_privs
CONNECT BY grantee = prior
granted_rolestart
WITH grantee IN
('DBA', 'PUBLIC');
```

44 Rollen
527 System Privilegien



Resource Rolle

RESOURCE	Provides the following resource-related system privileges: • CREATE ANALYTIC VIEW • CREATE ATTRIBUTE DIMENSION • CREATE CLUSTER • CREATE HIERARCHY • CREATE INDEXTYPE • CREATE MATERIALIZED VIEW • CREATE OPERATOR • CREATE PROCEDURE • CREATE PROPERTY GRAPH • CREATE SEQUENCE Be aware that RESOURCE no longer provides the UNLIMITED TABLESPACE system privilege. This role is provided for compatibility with previous releases of Oracle Database. You can determine the privileges encompassed by this role by querying the DBA_SYS_PRIVS data dictionary view. **Note:** Oracle recommends that you design your own roles for database security rather than relying on this role. This role may not be created automatically by future releases of Oracle Database.

Note: Oracle recommends that you design your own roles for database security rather than relying on this role. This role may not be created automatically by future releases of Oracle Database.

Oracle Database 23c Security Guide

Common Role

- Rolle wird in der CDB definiert und ist automatisch in allen PDBs verfügbar
- Privilegien in den PDBs können unterschiedlich sein
- Voraussetzung: Role beginnt mit “C##“ (Serverparameter)

```
SQL> CREATE ROLE c##dba CONTAINER=ALL;

Role created.

SQL> GRANT CREATE SESSION, ALTER SESSION TO c##dba CONTAINER=ALL;

Grant succeeded.
```

Vorschlag 2

- Eigene Rollen anlegen
- Beispiel:
  - `<FIRMENKÜRZEL>_DBA`
  - `<FIRMENKÜRZEL>_SCHEMA / <FIRMENKÜRZEL>_RESOURCE`
  - `<FIRMENKÜRZEL>_CONNECT`
- Bei Multitenant (Common Roles)
  - `C##<FIRMENKÜRZEL>_DBA`
  - `C##<FIRMENKÜRZEL>_SCHEMA / <FIRMENKÜRZEL>_RESOURCE`
  - `C##<FIRMENKÜRZEL>_CONNECT`
- Bei NON-CDB kann man keine Rollen anlegen, die mit C## beginnen

Passwort Komplexität

- Oracle Skript `$ORACLE_HOME/rdbms/admin/catpvf.sql`
- Erstellt 7 Verifizierungsfunktionen und ein zusätzliches Profile
  - `ora_complexity_check`
  - `ora_string_distance`
  - `ora12c_verify_function`
  - `verify_function_11G`
  - `verify_function`
  - `ora12c_strong_verify_function`
  - `ora12c_stig_verify_function + ora_stig_profile`
- Tipp: nicht direkt verwenden, sondern eigene auf dieser Basis erstellen

Common Profile

- Profiles werden auf CDB-Ebene gesetzt
- C## als Prefix

```
SQL> CREATE PROFILE c##techuser LIMIT
        FAILED_LOGIN_ATTEMPTS 5
        PASSWORD_LIFE_TIME 60
        PASSWORD_REUSE_TIME 60
        PASSWORD_REUSE_MAX 5
        PASSWORD_VERIFY_FUNCTION meine_verify_function
        PASSWORD_LOCK_TIME 1/24
        PASSWORD_GRACE_TIME 10
        INACTIVE_ACCOUNT_TIME 30;
```

Vorschlag

- Eigene Profiles verwenden
  - Wesentlich für die Passwortkomplexität / Alterung
- Beispiel:
  - `C##_<FIRMENKÜRZEL>_TECH_PROFILE`
  - `C##_<FIRMENKÜRZEL>_PERS_PROFILE`
  - `C##_<FIRMENKÜRZEL>_TEMP_PROFILE`
- Es gibt wenig Gründe, warum man bei der Multitenant Datenbank lokale Profiles verwenden sollte.
  - Kann allerdings bei Migrationen vorkommen

Schema Only Account

- Seit Version 18

1. Anlegen eines „normalen“ Users

```
GRANT create session TO johannes IDENTIFIED BY manager;
```

2. Anlegen eines Schema Only Accounts ohne Passwort

```
CREATE USER besitzer NO AUTHENTICATION QUOTA UNLIMITED ON users;
GRANT create session, create table, create sequence TO besitzer;
```

3. Zugriff auf Objekte für den normalen User zulassen:

```
ALTER USER besitzer GRANT CONNECT THROUGH johannes;
```

4. Anmeldung an den User mit zugehörigem Schema

```
sqlplus johannes[besitzer]/<passwort>@<TNS-Alias>
```

Privilege Capture

- Seit 12c
- Least Privilege Analyse
- Datenbank Package mit folgenden Prozeduren:
  - `CREATE_CAPTURE` → Erstellt eine Analysepolicy
    - Unterschiedliche Granularitäten (z.B. Datenbank, Rolle, Context)
  - `ENABLE_CAPTURE` → Aktivitiert die Policy und damit die Messung
  - `DISABLE_CAPTURE` → Deaktiviert die Policy
  - `GENERATE_RESULTS` → Erstellt die Datenbank Views
    - Z.B. `dba_used_sysprivs, dba_unused_sysprivs`
  - `DROP_CAPTURE` → Löscht die Analysepolicy

Lock Accounts

Locked Accounts

```
SQL> SELECT username, account_status FROM dba_users order by 1;

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
ANONYMOUS                      LOCKED
APPQOSSYS                      LOCKED
AUDSYS                         LOCKED
C##JOHANNES                    OPEN
…
REMOTE_SCHEDULER_AGENT         LOCKED
SYS                            LOCKED
SYS$UMF                        LOCKED
SYSBACKUP                      LOCKED
SYSDG                          LOCKED
SYSKM                          LOCKED
SYSRAC                         OPEN
SYSTEM                         OPEN
WMSYS                          LOCKED
XDB                            LOCKED
XS$NULL                        LOCKED
```

Lock Oracle Accounts

```
SQL> SELECT username, account_status FROM dba_users
      WHERE oracle_maintained='Y' AND account_status != 'LOCKED';

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
SYSTEM                         OPEN
SYSRAC                         OPEN
```

```
SQL> ALTER USER system ACCOUNT LOCK;

User altered.

SQL> ALTER USER system ACCOUNT LOCK;
ALTER USER sysrac ACCOUNT LOCK
*
ERROR at line 1:
ORA-28222: Operations cannot be performed on reserved user XS$NULL.
```

Lock Oracle Accounts

```
SQL> ALTER USER system ACCOUNT LOCK;
ALTER USER sysrac ACCOUNT LOCK
*
ERROR at line 1:
ORA-28222: Operations cannot be performed on reserved user XS$NULL.
```

SOLUTION

It's not allowed to lock (and unlock) SYSRAC and the authentication type cannot be changed, ONLY is allowed OS Authentication for SYSRAC.

Lock User Sys

```
SQL*Plus: Release 23.0.0.0.0 - Developer-Release on Tue Nov 14 23:52:28 2023
Version 23.2.0.0.0
Copyright (c) 1982, 2023, Oracle.  All rights reserved.
Connected to:

Oracle Database 23c Free, Release 23.0.0.0.0 - Developer-Release
Version 23.2.0.0.0

SQL> alter user sys account lock;
alter user sys account lock
*
ERROR at line 1:
ORA-40365: cannot lock SYS user in current password file format

% orapwd describe file=$ORACLE_HOME/dbs/orapwFREE
Password file Description : format=12
```

Wallet

Wallet Lizenzierung

- An Oracle Wallet is a PKCS#12 container used to store authentication and encryption keys. The Oracle database secure external password store feature stores passwords in an Oracle Wallet for password-based authentication to the Oracle database. The Oracle Wallet may also be used to store credentials for PKI authentication to the Oracle Database, configuration of network encryption (SSL/TLS), and Oracle Advanced Security transparent data encryption (TDE) master encryption keys. Network encryption (native network encryption, network data integrity, and SSL/TLS) and strong authentication services (Kerberos, PKI, and RADIUS) are no longer part of Oracle Advanced Security and are available in all licensed editions of all supported releases of Oracle Database.

Oracle Database 23c Database Licensing Information User Manual

1. TNS-Alias erstellen

- Tipp: Größere tnsnames.ora einfach per `ifile` erweitern

```
% cat tnsnames.ora
ifile=/opt/oracle/admin/network/tnsnames_wallet.ora

CARLOS23 =
   (description =
      (address = (protocol=tcp)(port=1521)(host=192.168.56.12))
   (CONNECT_DATA =
      (SERVICE_NAME = CARLOS)))
```

```
% cat /opt/oracle/admin/network/tnsnames_wallet.ora
JOHANNES_CARLOS23 =
   (description =
      (address = (protocol=tcp)(port=1521)(host=192.168.56.12))
   (CONNECT_DATA =
      (SERVICE_NAME = CARLOS)))
```

2. Wallet erstellen

```
% mkdir -p /opt/oracle/admin/wallet

% mkstore -wrl /opt/oracle/admin/wallet -create
Oracle Secret Store Tool Release 23.2.0.0.0 - Production
Version 23.2.0.0.0
Copyright (c) 2004, 2023, Oracle and/or its affiliates. All rights reserved.

Enter password:
Enter password again:

% mkstore -wrl `pwd` -createCredential JOHANNES_CARLOS23 JOHANNES manager
```

- Tipp: Bei Oracle Domains zwei Credentials pro Connect

3. sqlnet.ora anpassen

```
cat sqlnet.ora
wallet_location =
   (SOURCE =
      (METHOD = FILE)
      (METHOD_DATA =
          (DIRECTORY = /opt/oracle/admin/wallet)))
SQLNET.WALLET_OVERRIDE = TRUE
```

4. Ausprobieren

```
sqlplus /@JOHANNES_CARLOS23

SQL*Plus: Release 23.0.0.0.0 - Developer-Release on Wed Nov 15 01:47:45 2023
Version 23.2.0.0.0

Copyright (c) 1982, 2023, Oracle.  All rights reserved.

Last Successful login time: Wed Nov 15 2023 01:45:23 +01:00

Connected to:
Oracle Database 23c Free, Release 23.0.0.0.0 - Developer-Release
Version 23.2.0.0.0

SQL>
```

Valid Node Checking

Valid Node Checking

- Blacklist und Whitelist für Oracle Net
  - IP-Adresse, Range, Netzwerk-Segment
  - Bei Änderungen muss der Listener neu gestartet werden!

```
% cat sqlnet.ora
TCP.VALIDNODE_CHECKING=YES
TCP.EXCLUDED_NODES=(192.168.56.108)
```

```
sqlplus.exe johannes/manager@JOHANNES_CARLOS23

SQL*Plus: Release 19.0.0.0.0 - Production on Mi Nov 15 15:38:54 2023
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

ERROR:
ORA-12547: TNS: Verbindung verloren
```

Unified Auditing

Audit Policy

- Grundaufbau Audit Policy

Audit Schema und Rollen

- Schema AUDSYS
- Rollen
  - Audit Viewer Rolle
    - Audit Daten ansehen
  - Audit Admin Rolle
    - Policies verwalten
    - Audit Daten verwalten

Audit Viewer Role

Audit Daten ansehen

Audit Admin Role

Audit Daten verwalten

Policies verwalten

Kernel Relink

```
SELECT parameter, value from v$option
 WHERE parameter = 'Unified Auditing';

PARAMETER                      VALUE
------------------------------ ----------

Unified Auditing               FALSE
```

- Besagt nur, dass Unified Auditing nicht exklusiv benutzt wird, sondern das „alte“ Auditing ebenfalls genutzt werden kann (Mixed Mode)!
- Durch Kernel Relink kann das „alte“ Auditing ausgeschaltet werden

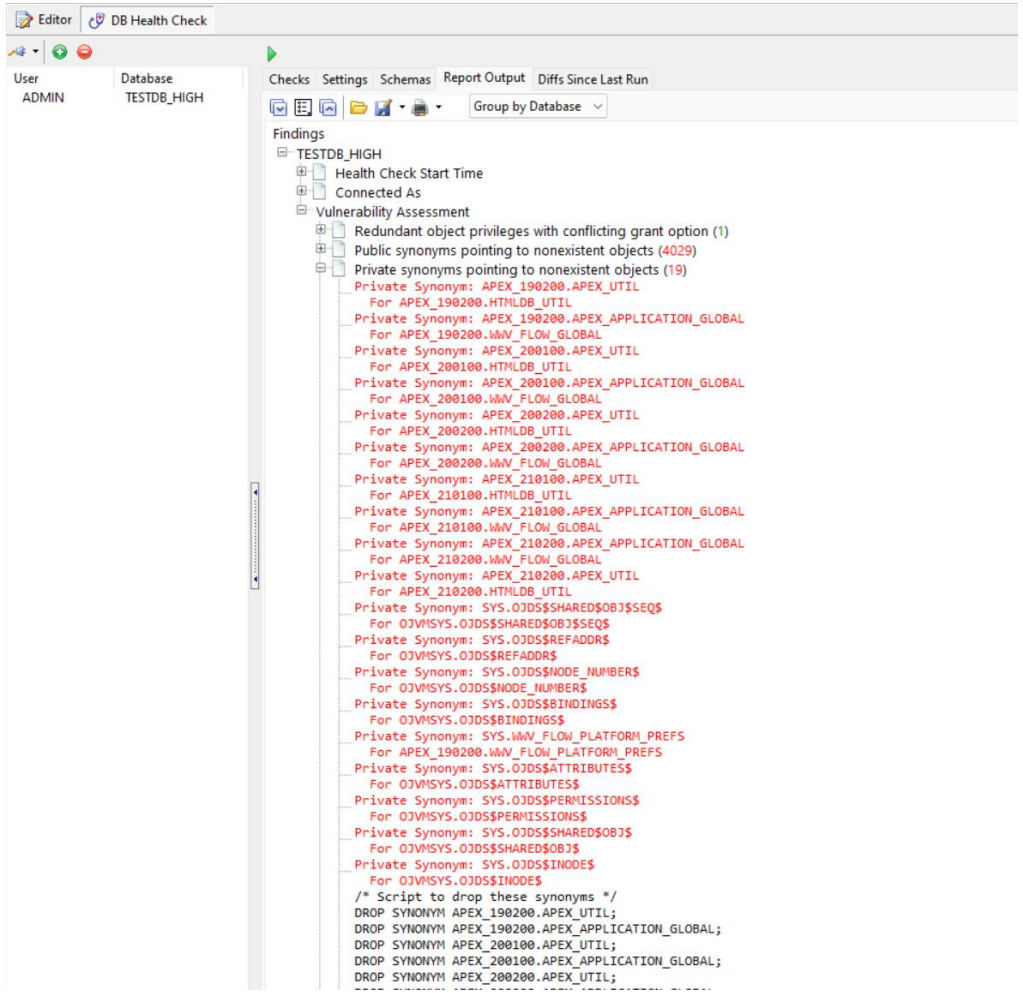
- Datapatch may be slower when Traditional and Unified Auditing are on
  https://mikedietrichde.com/2023/04/11/datapatch-may-be-slower-when-traditional-and-unified-auditing-are-on/

12c Auditing – Audit Policy

- Grundaufbau 12c Audit Policy

Kontrolle

- DBSAT → gibt es scheinbar nicht mehr
- Toad Health Check
- …



Kontakt

CarajanDB GmbH
Siemensstraße 25
50374 Erftstadt

www.carajandb.com
johannes.ahrends@carajandb.com

☎ +49 (22 35) 1 70 91 84
+49 (1 70) 4 05 69 36

Social Media:
@carajandb
johannes.ahrends
Carajandb
carajandb