Oracle Database 18c Release 1

Neue Funktionalitäten zur Datenbank-Sicherheit

Norman Sibbing (Norman.Sibbing@oracle.com)

BU Core & Cloud Technologies
Oracle Deutschland B.V. & Co KG

ORACLE

Oracle Database 18.1 Security Feature Updates

Agenda

1. Oracle Database Core Updates
2. Multitenant Databases
3. Oracle Advanced Security
4. Centrally Managed Users with Microsoft Active Directory

Oracle Database 18.1 Security Feature Updates

Agenda

1. Oracle Database Core Updates
2. Multitenant Databases
3. Oracle Advanced Security
4. Centrally Managed Users with Microsoft Active Directory

Oracle Database Security Core Updates

Schema Only Accounts

- CREATE USER Benutzer IDENTIFIED BY ‘Geheim‘;
  - Authentifizierung durch die Datenbank (Passwort)
- CREATE USER Benutzer IDENTIFIED EXTERNALLY;
  - Authentifizierung durch das Betriebssystem (OS-Authentifizierung, Kerberos, PKI)
- CREATE USER Benutzer IDENTIFIED GLOBALLY;
  - Authentifizierung über ein Identitity Management System (Enterprise User Security)
- **Neu: CREATE USER Benutzer NO AUTHENTICATION;**
  - Es existiert keine Authentifizierungsmethode
  - Nicht anwendbar bei Benutzern mit SYS* Administrations-Privilegien und bei Database Links

* SYSDBA, SYSKM, SYSOPER, SYSBACKUP, SYSDG, SYSRAC

Oracle Database Security Core Updates

12c - Obfuscated Sensitive Credential Data in the Data Dictionary

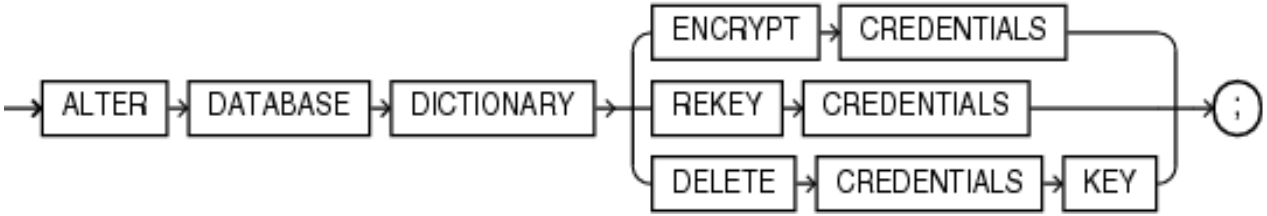
- Für Datenbank-Links und Scheduler-Jobs werden die Passwörter „verschleiert“ -obfuscated- gespeichert
- „Verschleierte“ Passwörter lassen sich über die Data Dictionary Tabellen SYS.LINK$ und SYS.SCHEDULER$_CREDENTIAL auslesen

```
SQL> select PASSWORDX from SYS.LINK$;

PASSWORDX
--------------------

07AAA610A6F5486F00E56453E8963C05BCDBE509D682E23FB8662FC67A764571552C50ECBA4E8A243F386398E003C6EF997CC7AA96E592DF43FA3802CEB40F93E8ECBC57D9AA72A672086B7788119A965B5C95D663736CBC1D9DE2B3849015E69058DF79907B27034ECA3424D12D82CBDD71566A8CD86802A1A51203760D550
```

Oracle Database Security Core Updates

18c - Encrypt Sensitive Credential Data in the Data Dictionary

- Echte Verschlüsselung der Anmeldeinformationen in den SYS.LINK$ und SYS.SCHEDULER$_CREDENTIAL Tabellen



- Ähnlich zur Verschlüsselung von Spalten und Tablespaces mittels TDE
  - Eine Advanced Security Option-Lizenz wird hierfür jedoch nicht benötigt und steht in allen Editionen ab Oracle 18c zur Verfügung
- Der Keystore (Wallet) muss geöffnet sein

Oracle Database Security Core Updates

Oracle Data Pump und verschlüsselte Database-Links Passwörter

- Passwörter werden jedes Mal beim Export bzw. Import gegen “Dummies” ausgetauscht
  - Dokumentation: Known invalid password
- ORA-39395: Warning: object TEST.LOOPBACK requires password reset after import

Oracle Database Security Core Updates

Write Unified Audit Trail Records to SYSLOG or the Windows Event Viewer

- UNIFIED_AUDIT_SYSTEMLOG = 'facility_clause.priority_clause‘ | true/false
- Nicht alle Informationen stehen im SYSLOG / Event Viewer zur Verfügung

```
Apr 16 09:06:50 tde Oracle Unified Audit[11188]: LENGTH: '156' TYPE:"4"
DBID:"946366664" SESID:"2439550631" CLIENTID:"" ENTRYID:"1" STMTID:"1"
DBUSER:"SYS" CURUSER:"SYS" ACTION:"100" RETCODE:"1017" SCHEMA:"" OBJNAME:""
```

- Detailinformationen befinden sich im Datenbank Audit Trail

```
SQL> select OS_USERNAME,DBUSERNAME,CLIENT_PROGRAM_NAME,AUDIT_TYPE from
unified_audit_trail where sessionid=2439550631 and statement_id=1;

OS_USERNAME    DBUSERNAME    CLIENT_PROGRAM_NAME       AUDIT_TYPE
-------------- ------------ ------------------------ --------------------

oracle          SYS           sqlplus@tde (TNS V1-V3)  Standard
```

Oracle Database Security Core Updates

Sonstige Neuerungen

- Mehr Kontrolle durch neue SQL*Net TLS/SSL Parameter
  - ADD_SSLV3_TO_DEFAULT
    - True/False: Erlaubt/Verbietet die Verwendung von SSLv3
  - ACCEPT_MD5_CERTS und ACCEPT_SHA1_CERTS
    - True/False: Erlaubt/Verbietet die Verwendung der MD5 bzw. SHA1 Algorithmen
- Import und Export des Unified Audit Trails mit Oracle Data Pump
  - expdp mit INCLUDE=AUDIT_TRAILS Parameter
- AS ENCRYPTED und AS DECRYPTED Klausel für RMAN DUPLICATE
  - Oracle Cloud DB -> On-Premises DB bzw. On-Premises DB -> Oracle Cloud DB
- Read-only Oracle Home Support
  - Instanz-spezifische Dateien werden außerhalb des Oracle-Homes gespeichert

Oracle Database 18.1 Security Feature Updates

Agenda

1. Oracle Database Core Updates
2. Multitenant Databases
3. Oracle Advanced Security
4. Centrally Managed Users with Microsoft Active Directory

Multitenant Databases*

Pluggable Databases erhalten getrennte/isolierte Keystores

- Datenbank Initialisierungsparameter WALLET_ROOT

```
ALTER SYSTEM SET WALLET_ROOT="wallet-root" SCOPE=SPFILE;
```

- Der Parameter beschreibt das Keystore-Basis-Verzeichnis
  - Struktur: /wallet-root/pdb-guid/tde

```
wallet-root/tde/ewallet.p12
wallet-root/tde/ewallet_20161209183336444.p12
wallet-root/3FD1C95B48205D0FE053C5A0E40AEF8C/tde/ewallet.p12
```

- Ersetzt den Parameter SQLNET.ENCRYPTION_WALLET_LOCATION
  - Gilt auch für Non-CDBs

*A restricted use license is included with all Oracle Database offerings that permits you to use the container database architecture in single-tenant mode without the Oracle Multitenant option license.

Multitenant Databases

Pluggable Databases erhalten getrennte/isolierte Keystores

- Datenbank Initialisierungsparameter TDE_CONFIGURATION*

```
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=FILE" SCOPE=both;
```

- Zur Auswahl stehen folgende Typen von Keystores
  - FILE: Das klassische Wallet
  - HSM: Hardware Security Modul
  - OKV: Oracle Key Vault
- Jede PDB kann unterschiedlichen Keystore-Typ verwenden
- WALLET_ROOT muss vorab gesetzt werden

*Dieser Parameter kann nur in einer Oracle Database Enterprise Edition auf Engineered Systems und ab Oracle Database Cloud Service Enterprise Edition aufwärts verwendet werden

Oracle Database 18.1 Security Feature Updates

Agenda

1. Oracle Database Core Updates
2. Multitenant Databases
3. Oracle Advanced Security
4. Centrally Managed Users with Microsoft Active Directory

Oracle Advanced Security

Bring your own key: User-Defined Master Encryption Key

- Verwendung eines Master Encryption Keys (MEK), der außerhalb der Datenbank generiert wurde (z.B. Key-Management System)
- **ADMINISTER KEY MANAGEMENT** mit **CREATE ENCRYPTION KEY** Klausel
  - ADMINISTER KEY MANAGEMENT CREATE ENCRYPTION KEY '[mkid:mk | mk]' IDENTIFIED BY keystore_password;

```
ADMINISTER KEY MANAGEMENT CREATE ENCRYPTION KEY
'10203040506070801112131415161718:3D432109DF88967A541967062A6F4E460E892318E3
07F017BA048707B402493C' IDENTIFIED BY keystore_password;
```

- Aktivierung des neuen Master Encryption Keys
  - ADMINISTER KEY MANAGEMENT USE KEY ‘mkid’ IDENTIFIED BY keystore_password
  - mkid = SELECT KEY_ID FROM V$ENCRYPTION_KEYS;

Oracle Database 18.1 Security Feature Updates

Agenda

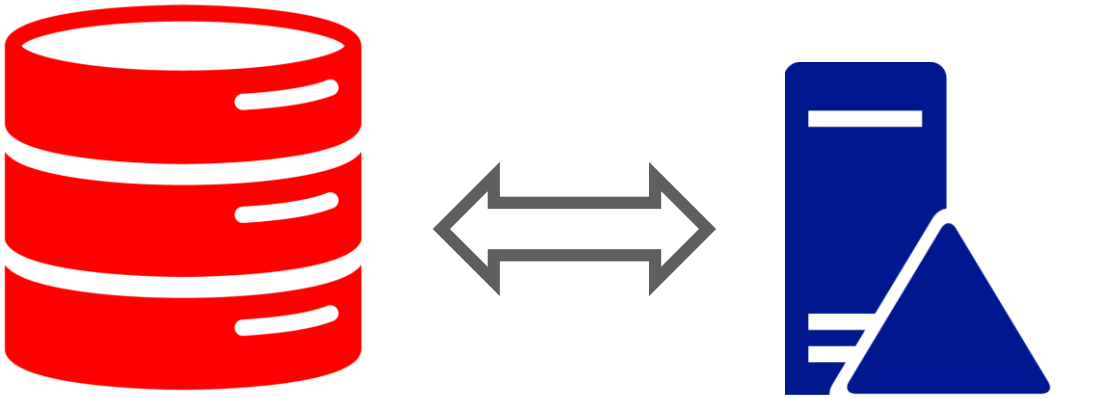
1. Oracle Database Core Updates
2. Multitenant Databases
3. Oracle Advanced Security
4. Centrally Managed Users with Microsoft Active Directory

Active Directory Integration mit Enterprise User Security

Bis Oracle Datenbank 12.2

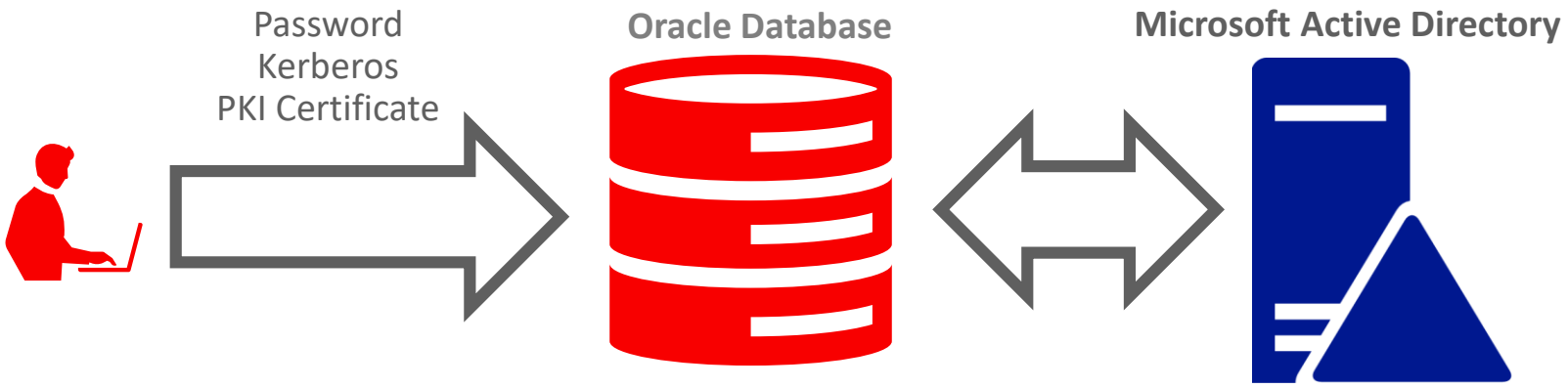
Centrally Managed Users mit Microsoft Active Directory

18c: Konzept



Centrally Managed Users mit Microsoft Active Directory

Authentifikation



Centrally Managed Users mit Microsoft Active Directory

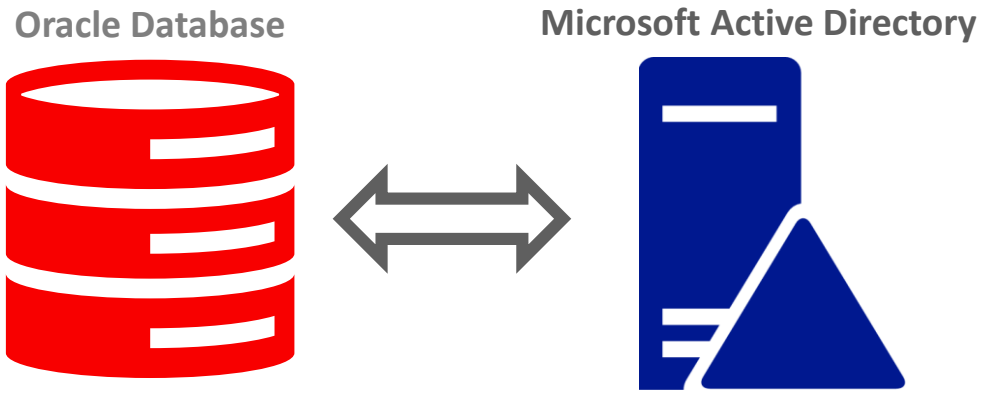
Oracle Passwort Filter

Microsoft Active Directory

- Oracle Werkzeug
  - Installiert Oracle Database Passwort Filter
  - Erweitert AD Schema
- Oracle Database Passwort Filter
  - Generiert Datenbank-Benutzer Passwort bei Änderung des AD Passwortes

Centrally Managed Users mit Microsoft Active Directory

Unterstützung der Active Directory Account Policies



- Passwort Policy
- Kerberos Policy
- Lockout Policy

Centrally Managed Users mit Microsoft Active Directory

Autorisierung

Oracle Database

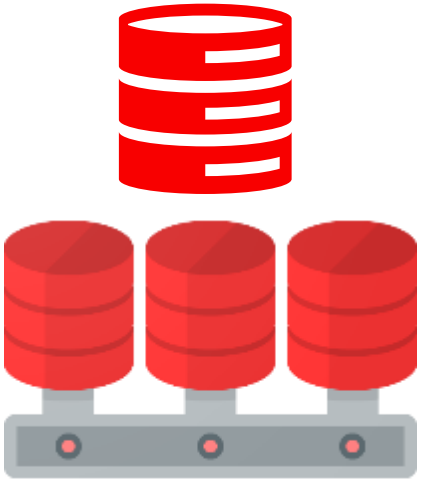
Oracle Database
Users and Groups

Active Directory

Active Directory
User and Groups

- 1:1 User Mapping
- Shared Schema Mapping
- Rolen Mapping
- Administrative Benutzer

TNS-Namensauflösung mit Active Directory

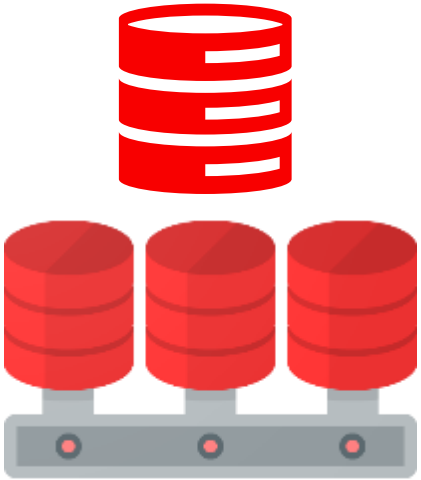


Net Naming Services

Centrally Managed Users

Active Directory Forest

Kombination möglich



Net Naming Services

Centrally Managed Users

Oracle Directory Services

Active Directory Forest

Fazit

18c ORACLE Database

- Weiterentwicklung bestehender Sicherheits-Funktionen
- Neue Funktion wie das Centrally Managed Users (CMU)
- Verbesserung der Datenbank-Sicherheit
- Jährliche Releases verbessern Reaktionsmöglichkeit auf aktuelle Gefahren
- Neue Funktionen zuerst in der Oracle Cloud verfügbar und testbar

ORACLE

Oracle Database Security

- Deutsche Blogs: https://blogs.oracle.com/coretec/
- Oracle 18c Security: https://docs.oracle.com/en/database/oracle/oracle-database/18/security.html
- Oracle Security: https://www.oracle.com/security/index.html

Q & A

Connect With Us

/OracleDatabase

/OracleSecurity

blogs.oracle.com/
SecurityInsideOut

Oracle Database Insider

/Oracle/database

/OracleLearning

oracle.com/database/security

oracle.com/technetwork/database/security

Hardware and Software
Engineered to Work Together


ORACLE®