



Oracle AI Database Security 26ai New Features

Focusing on Major Security
Enhancements

Stefan Oehrli



The Oracle ACE Program

400+ technical experts helping peers globally



- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com



Stefan Oehrli – Modern Data Platforms

stefan.oehrli@accenture.com



Modern
Data
Platforms



Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
 - Security assessments and reviews
 - Database security concepts and their implementation
 - Oracle Backup & Recovery concepts and troubleshooting
 - Oracle Enterprise User and Advanced Security, DB Vault, ...
 - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)



oradba.ch



@stefanoehrli.bsky.social



@stefanoehrli



Oracle AI Database 26ai

What about the Security
Features in 26ai?

- 1 Introduction
- 2 SQL Firewall
- 3 Authentication
- 4 Authorization
- 5 Auditing
- 6 Encryption
- 7 Further Innovations
- 8 Conclusion

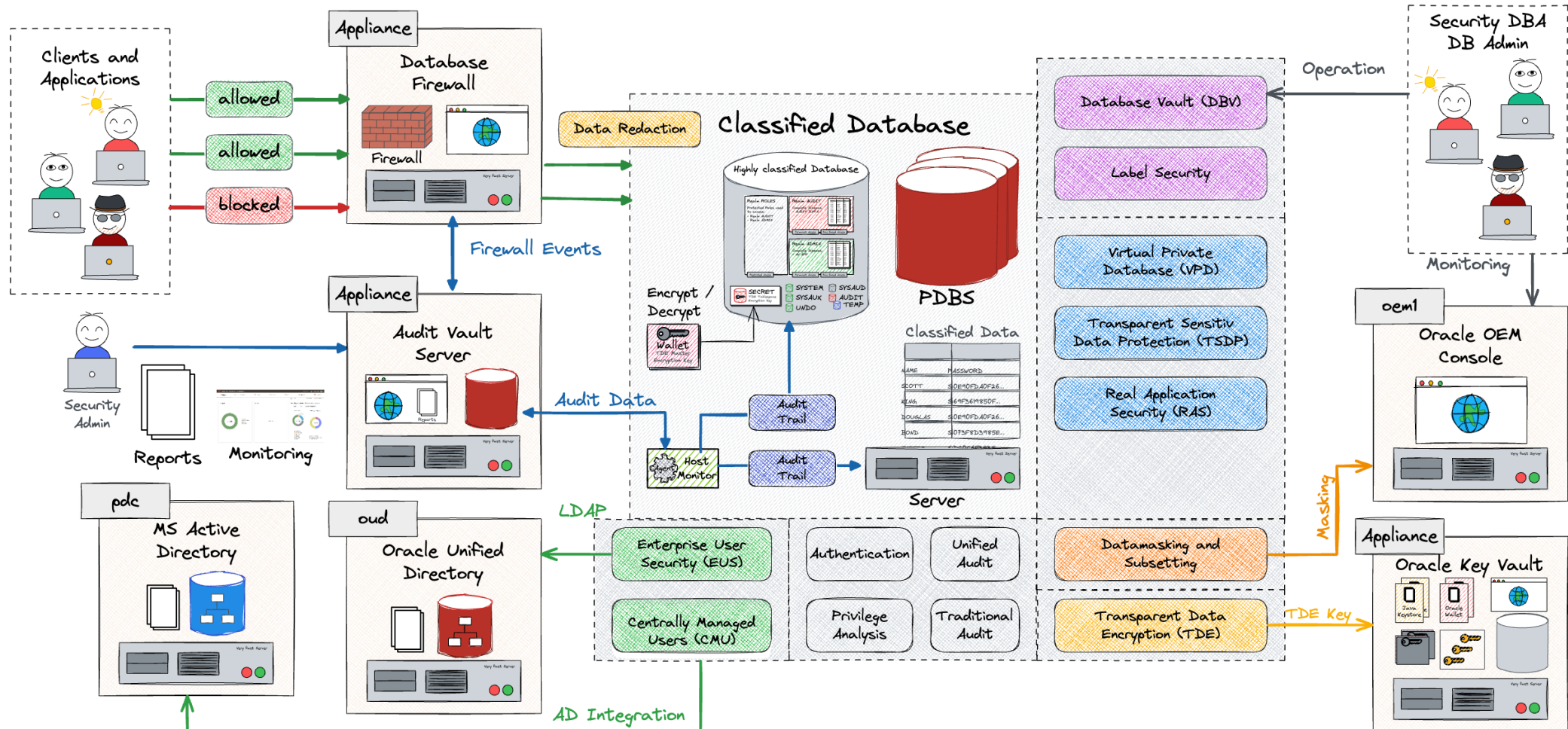
1

Introduction

What about the
Security Features in
26ai?

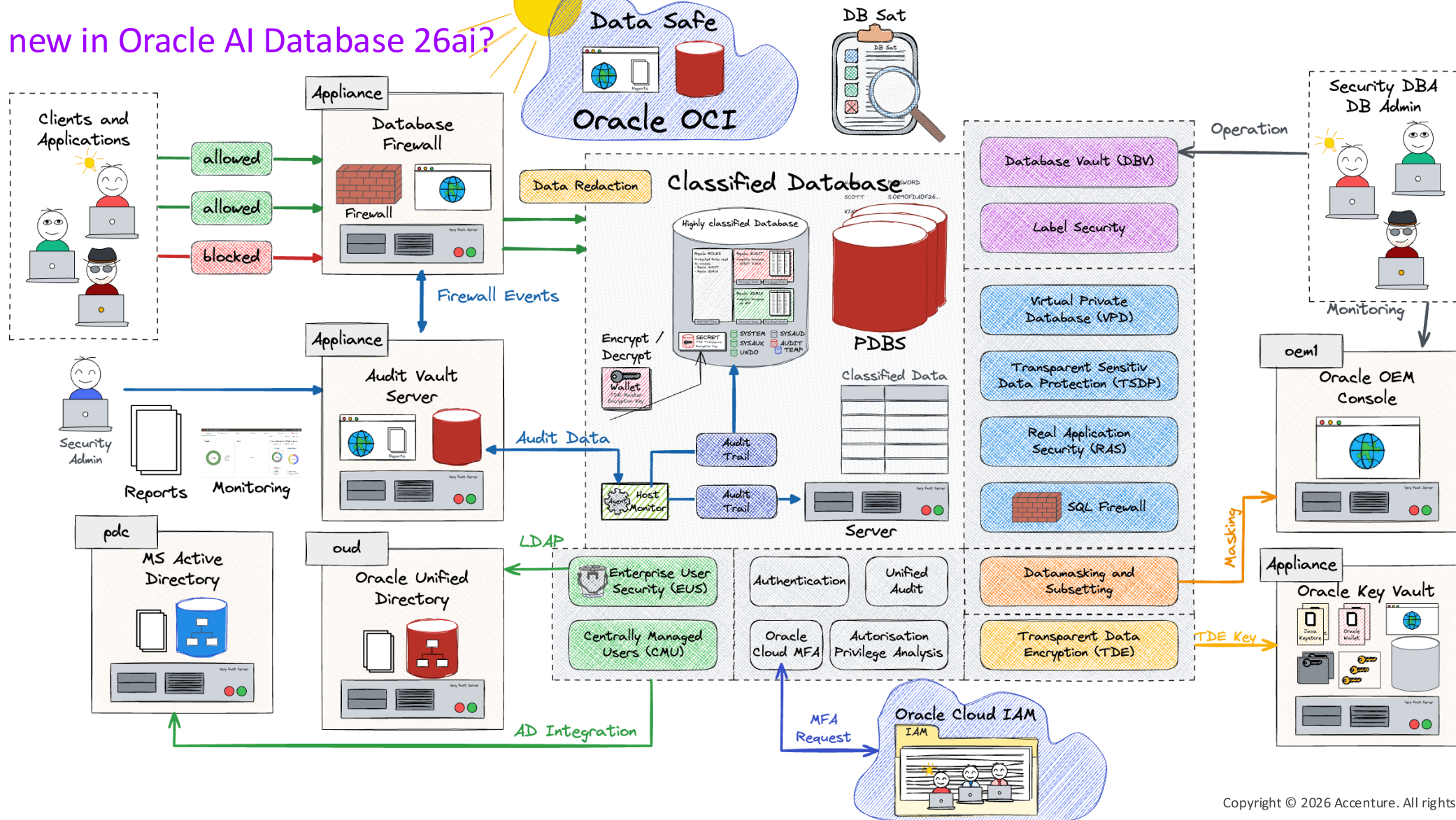
Maximal Database Security Architecture

What's new in Oracle AI Database 26ai?



Maximal Database Security Architecture

What's new in Oracle AI Database 26ai?



In a Nutshell

New Security Features in Oracle AI Database 26ai on the Horizon

Exploring New Frontiers

- SQL Firewall: A Major Leap in Database Security

Doing the Housework

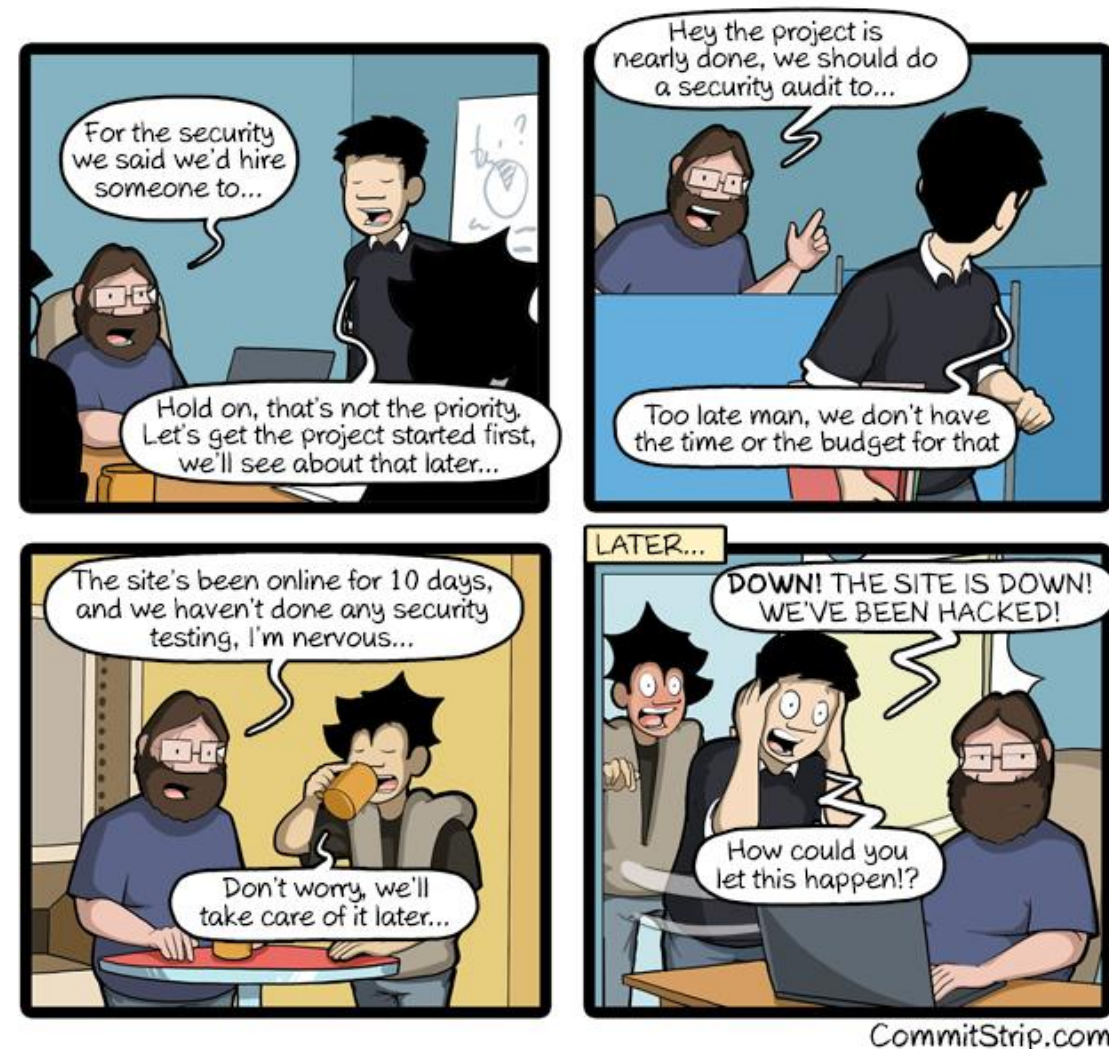
- Adapting to new standards for enhanced security
- Incremental upgrades in auth, audit, and encryption

Saying Farewell to Familiar Features

- Deprecation of Enterprise User Security (EUS)
- Desupport of Traditional Auditing
- Desupport of Case Insensitive Passwords

Areas of Continued Development

- Oracle AI Database specific features!?



2

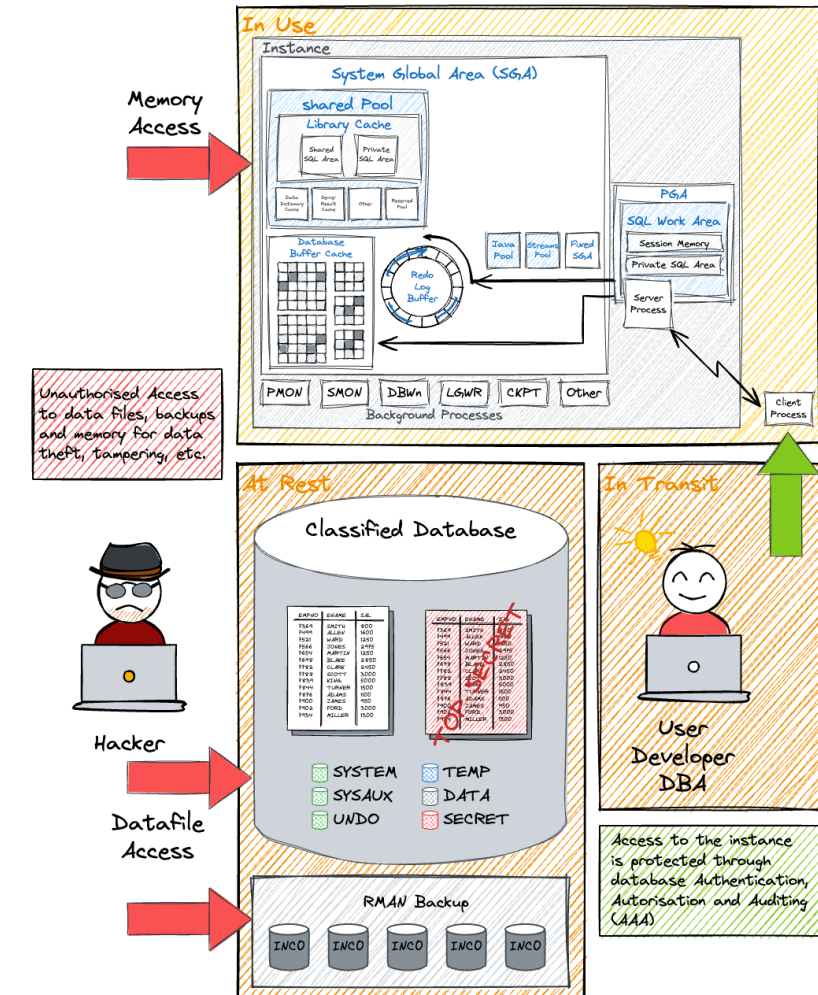
SQL Firewall

The latest Security
Achievement

The Security Challenges of a Database

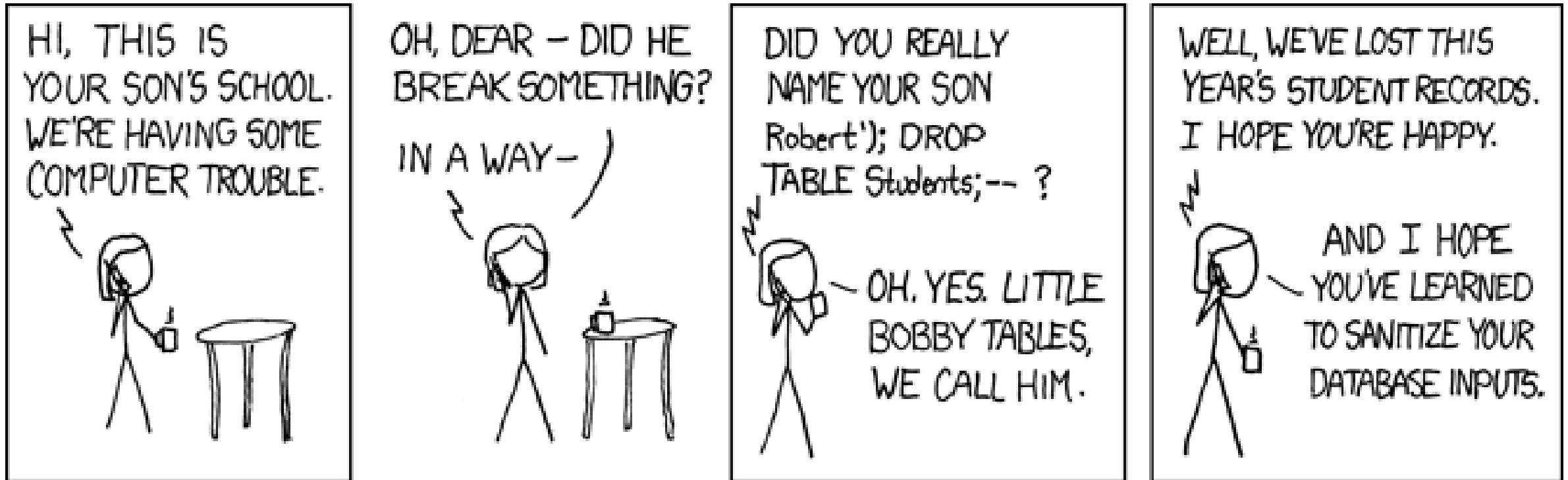
The dirty dozen...

- **Access Bypass:** Unpatched or misconfigured database vulnerabilities.
- **Privilege Abuse:** Exploiting application vulnerabilities for higher access.
- **Sensitive Data Search:** In unprotected systems and databases.
- **Credential Theft:** Via phishing, social engineering, or malware.
- **System Bridging:** Using less secure systems to target secure ones.
- **Password Exploitation:** Guessing or poor management.
- **SQL Injection:** Manipulating user input to exploit applications.
- **Rogue Accounts:** For reconnaissance and access escalation.
- **Non-Production Data Risks:** Targeting less secure dev/test environments.
- **Unencrypted Data Exposure:** Accessing or stealing files from disk or backups.



SQL Injection

Exploits of a Mom

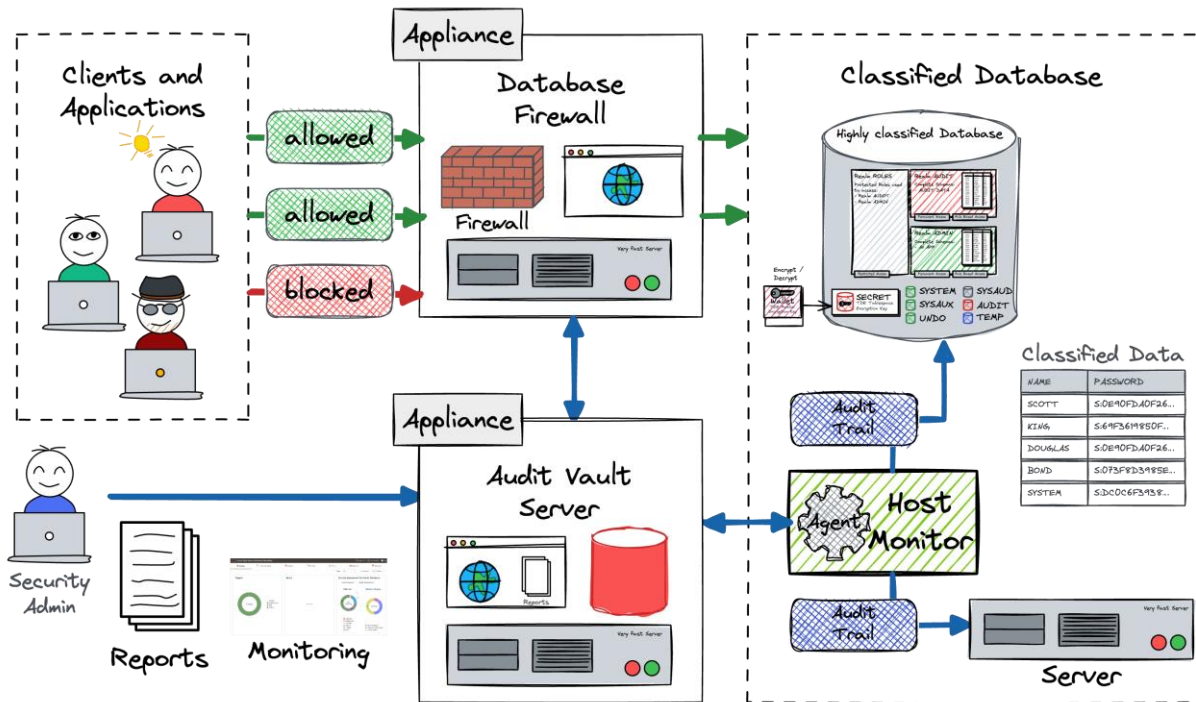


xkcd: <https://xkcd.com/327>

But we already have it, don't we?

Some kind of SQL firewall functionality

Oracle Audit Vault and Database Firewall



- Dedicated Product for central Audit Management and Reporting
- Two main Features
 - **Audit Vault Server** to control, manage, report
 - **Database Firewall** to monitors data access, enforces access policies
- Support a **wide range** of targets / databases
 - Oracle AI Database
 - Microsoft SQL Server
 - MySQL, PostgreSQL, MongoDB, IBM DB2
- Able to **log** and **block** database activities
- **Dedicate** Infrastructure
 - Requires corresponding system architecture

SQL Firewall Overview

What exactly is it about?

Real-Time Protection

- Blocks unauthorized SQL and preventing SQL injection and access anomalies

Customizable Allow-Lists

- Create specific SQL permissions for each user, with logging of unusual activities

Connection and Statement Control

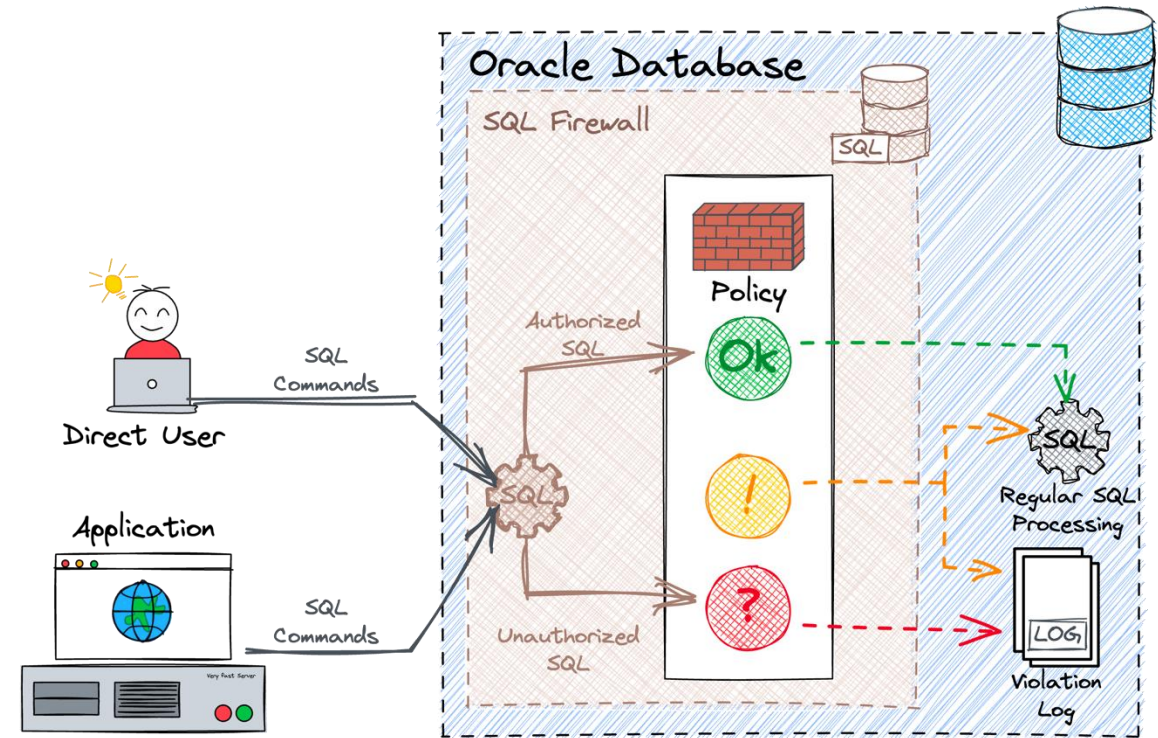
- Manages **allowed** SQL **statements** and **connection** paths, e.g. IP addresses, context etc.

Integrated into Oracle AI Database

- Ensures inspection of all SQL activities, including encrypted and network SQL

Flexible Policy Application

- Tailored policies for different database accounts, enhancing gradual security improvement



Navigating SQL Firewall – Processes

Understanding the Mechanics and Strategies for Optimal Deployment

Learning Stage

- **Capture** the user's SQL activities
- **Review** the capture
- **Generate** an allow-list

Protecting Stage

- **Enable** the allow-list
- **Monitor violations** SQL Firewall raises violation for any unexpected access patterns.



Navigating SQL Firewall - Usage

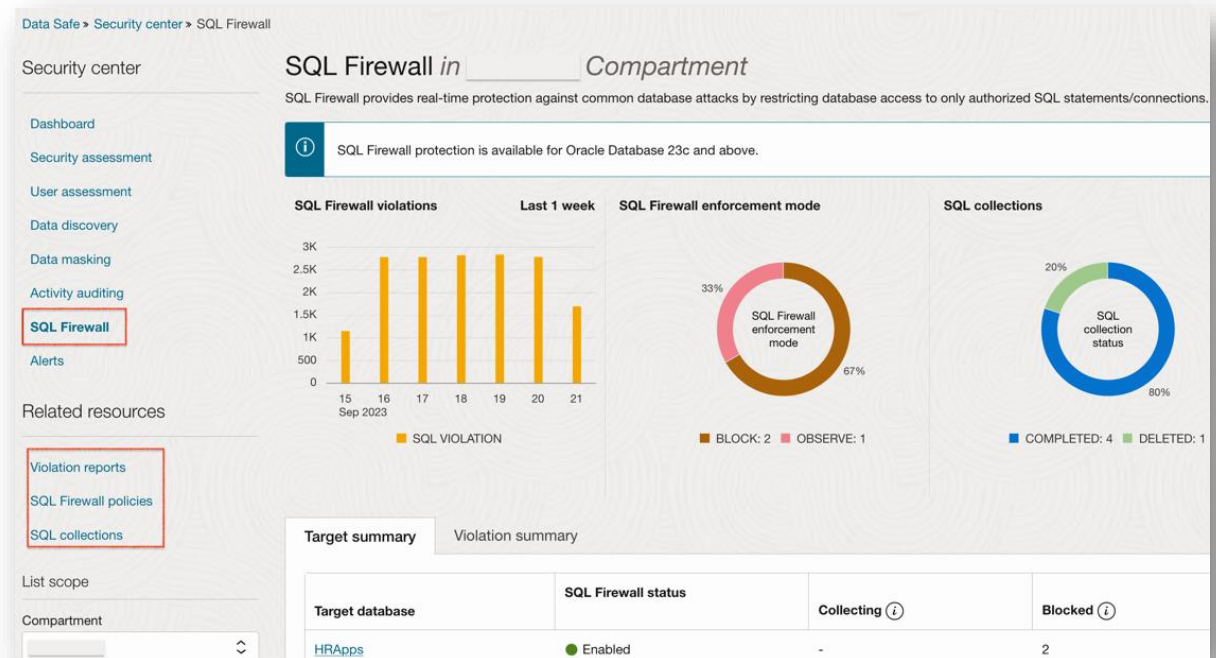
CLI or GUI you choose...

SQL Interface for the brave DBA

- System Privilege `ADMINISTER SQL FIREWALL`
- Predefined Roles
 - `SQL_FIREWALL_ADMIN`
 - `SQL_FIREWALL_VIEWER`
- Data Dictionary Views
- Violation Log `DBA_SQL_FIREWALL_VIOLATIONS`
- Capture Log `DBA_SQL_FIREWALL_CAPTURE_LOGS`
- A couple more `DBA_SQL_FIREWALL_`%
- Several base table in `SYSAUX` i.e.
`FW_CAPTURE$`, `FW_ALLOW_LIST$`,
`VIOLATION_LOG$`, ...

Oracle Data Safe on Oracle Cloud

- Manage multiple SQL Firewalls centrally
- Comprehensive view of SQL Firewall violations



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Connect as user with SQL_FIREWALL_ADMIN role
- Enable SQL Firewall

```
EXEC DBMS_SQL_FIREWALL.ENABLE;
```

- Check the status of the SQL Firewall

```
SELECT * FROM dba_sql_firewall_status;
```

STATUS	STATUS_UPDATED_ON	EXCLUDE_JOBS
-----	-----	-----
ENABLED	21.11.23 06:30:01.430118000 +01:00	Y

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Enable a capture for the user SCOTT

```
BEGIN
  DBMS_SQL_FIREWALL.CREATE_CAPTURE (
    username          => 'SCOTT',
    top_level_only    => TRUE,
    start_capture      => TRUE);
END;
/
```

- Verify what SCOTT is doing

```
SELECT sql_text FROM dba_sql_firewall_capture_logs
WHERE username = 'SCOTT';
```

SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Disable capture for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.STOP_CAPTURE ('SCOTT');
```

- Generate an allow-list for user SCOTT

```
EXEC DBMS_SQL_FIREWALL.GENERATE_ALLOW_LIST ('SCOTT');
```

- Query the allowed activity for user SCOTT

- DBA_SQL_FIREWALL_ALLOWED_IP_ADDR
- DBA_SQL_FIREWALL_ALLOWED_OS_PROG
- DBA_SQL_FIREWALL_ALLOWED_OS_USER
- DBA_SQL_FIREWALL_ALLOWED_SQL



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Customize the allow-list e.g. `DBMS_SQL_FIREWALL.ADD_ALLOWED_CONTEXT` and `DBMS_SQL_FIREWALL.DELETE_ALLOWED_CONTEXT`
- Enable the allow-list using `DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST`

```
BEGIN
  DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST (
    username      => 'SCOTT',
    enforce       => DBMS_SQL_FIREWALL.ENFORCE_SQL,
    block         => TRUE);
END;
/
```

- Start having fun with the protected Database...



SQL Firewall - Quick start

Short Journey through the SQL Firewall Configuration

- Limited availability of SCOTT

```
SQL> SELECT ename,sal FROM scott.emp WHERE ename='SCOTT';  
SELECT ename,sal FROM scott.emp WHERE ename='SCOTT'  
                                     *  
  
ERROR at line 1:  
ORA-47605: SQL Firewall violation
```

- Chooses wisely what and when to capture application activity

Beyond the Basics - SQL Firewall Insights

Key Considerations and Advanced Knowledge

Smooth integration with other Oracle products

- **Multitenant Environment** both the CDB root and the individual PDB levels are affected
- **Oracle Centrally Managed Users** capture global user's activities is supported
- **Oracle Scheduler** jobs are excluded by default
- **Oracle Database Vault** not verified
- **Oracle Data Pump** Export and Import supports different use cases
 - Export and import SQL Firewall captures and allow-lists metadata e.g. `INCLUDE=SQL_FIREWALL`
 - Consider Procedures `DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST` or `DBMS_SQL_FIREWALL.IMPORT_ALLOW_LIST` to transfer allow-list

3

Authentication

The "*Who's Who*" in the database

Authentication

No breaking news, just continuous improvement

- Increased **Maximum** Password Length
 - Passwords now can have up to 1024 bytes used to be 30 bytes
- **Desupport** of Case Insensitive Passwords i.e. legacy 10g Password hash
 - A Problem when a user only has a 10g password hash

```
SELECT username FROM dba_users WHERE ( password_versions = '10G ' OR  
password_versions = '10G HTTP ' )  
AND username <> 'ANONYMOUS';
```

- Clean up and adjust **Password Policies** i.e.g scripts `utlpwdmg.sql` and `catpvf.sql`
 - The Profile *ora_stig_profile* has now a password lifetime of 35days
 - Old verify function have been removed e.g. *verify_function_11G* and *verify_function*

Authentication

No breaking news, just continuous improvement

- Updated **Kerberos Library and Improvements**
 - KERBEROS5_CC_NAME supports multiple principals and stores in encrypted format
 - It provides cross-domain support for accessing resources in other domains.
 - It supports Windows Credential Guard
 - Kerberos on Database can search for the KERBEROS5_CC_PRINCIPAL
 - The okinit, oklist, and okdstry utilities work with encrypted cache
- **RADIUS Configuration Enhancement**
 - Supports for Requests for Comments (RFC) 6613 and 6614 guidelines



Deprecation of mkstore

Use orapki securestore for Secure External Password Store

- `mkstore` utility **deprecated**
- Previously used to manage **Secure External Password Store (SEPS)**
- SEPS functionality **remains unchanged**
- Credential management now handled by **orapki securestore**
- Aligns wallet and credential management with **Oracle PKI tools**

From mkstore to orapki securestore

Modern credential management for SEPS

■ Previous approach

```
mkstore -wrl $TNS_ADMIN/wallet -create
mkstore -wrl $TNS_ADMIN/wallet -createCredential LABPDB1 soug_test manager
mkstore -wrl $TNS_ADMIN/wallet -listCredential
```

■ Recommended approach

```
orapki wallet create -wallet $TNS_ADMIN/wallet -pwd LAB42SOUG -auto_login
orapki secretstore create_credential -wallet $TNS_ADMIN/wallet \
-pwd LAB42SOUG -connect_string LABPDB1 -username soug_test
-password manager
orapki secretstore list_credentials -wallet $TNS_ADMIN/wallet -pwd
LAB42SOUG
```



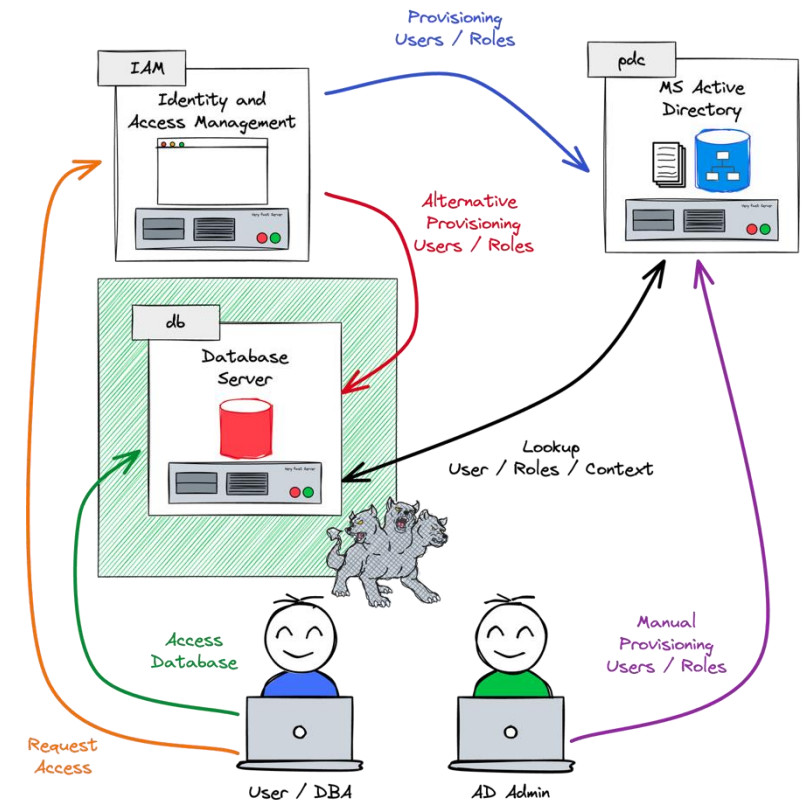
Deprecation Enterprise User Security (EUS)

It is time to say goodbye...

- Enterprise User Security (EUS) has been deprecated
 - No hurry, it will not be removed immediately
 - Consider next upgrade wisely
 - Along this *mkstore* is deprecated as well
 - *mkstore* functionality has been added to **orapki**

Alternatives?

- Oracle **Centrally Managed Users** (CMU)
 - ... does not require an additional Oracle directory
 - ... enables the administration of users directly in MS AD
 - ... does not require an additional license but
 - ... Supported only by Oracle Enterprise or Free Edition
- New **Microsoft Azure Active Directory Users** for Oracle Databases



Multi-Factor Authentication for Oracle Database

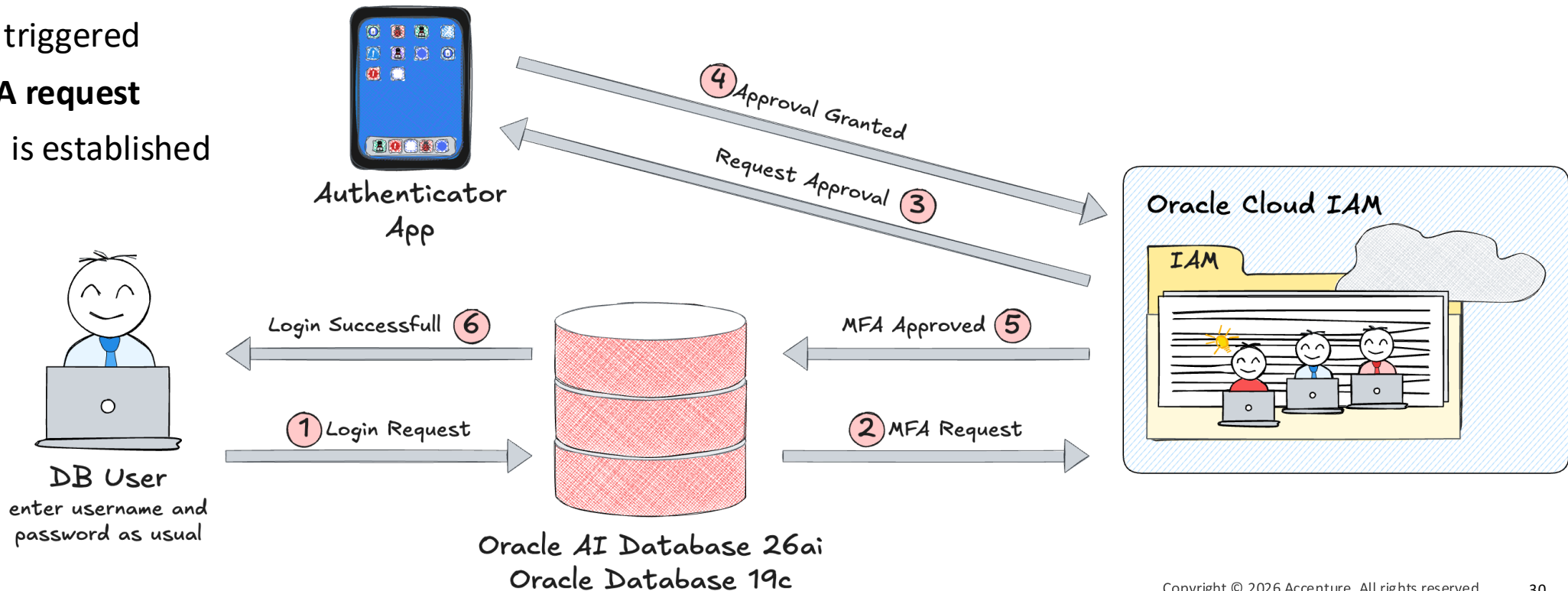
Stronger authentication for database access

- Native **Multi-Factor Authentication (MFA)** support
- Integrates with **OCI Identity Domains (IAM)**
- Adds a **second authentication factor** to database login
 - Does work for Cloud and on-premises databases as of Oracle Database 19.28 (July 2025)
- Supports **TOTP authenticator** apps. Ok the Oracle Authentication App 😊
- Protects **privileged and administrative database accounts**
- Still have a few limitations:
 - Can **not** be combined with CMU
 - Admin connections using external password file
 - Role passwords

Database Login with MFA

Authentication flow with OCI Identity Domains

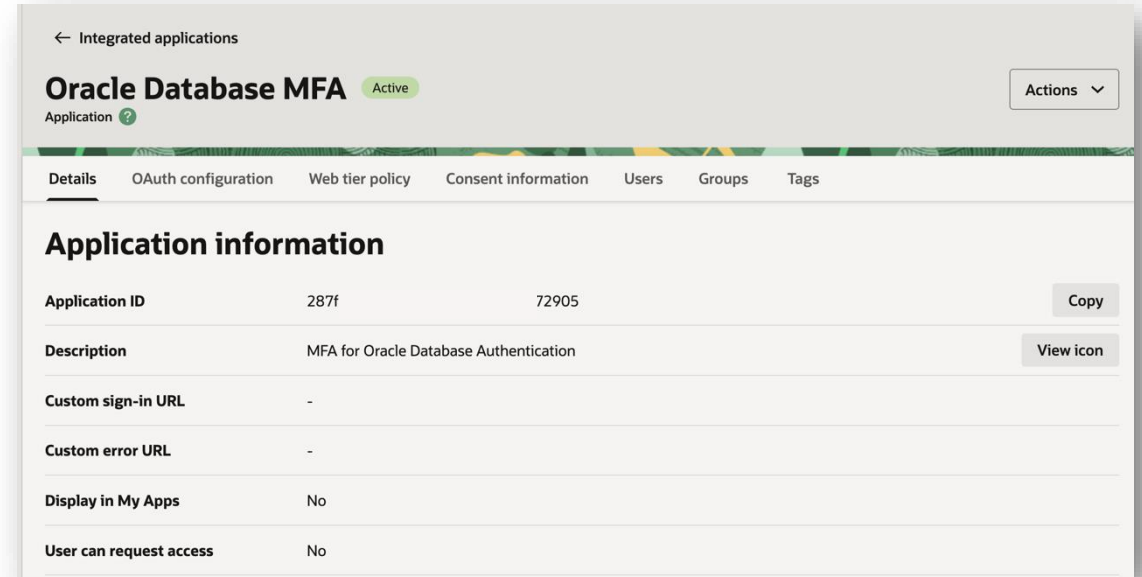
- User connects to the database client (SQL*Plus, SQLcl, tools)
- Database redirects authentication to **OCI Identity Domain**
- Identity Domain validates **password**
- MFA challenge is triggered
- User confirm **MFA request**
- Database session is established



Example Configuration

Enabling MFA authentication for a database user

- User mapped to OCI IAM identity
- Authentication managed by Identity Domain
- MFA policy configured in IAM
- Database trusts IAM authentication

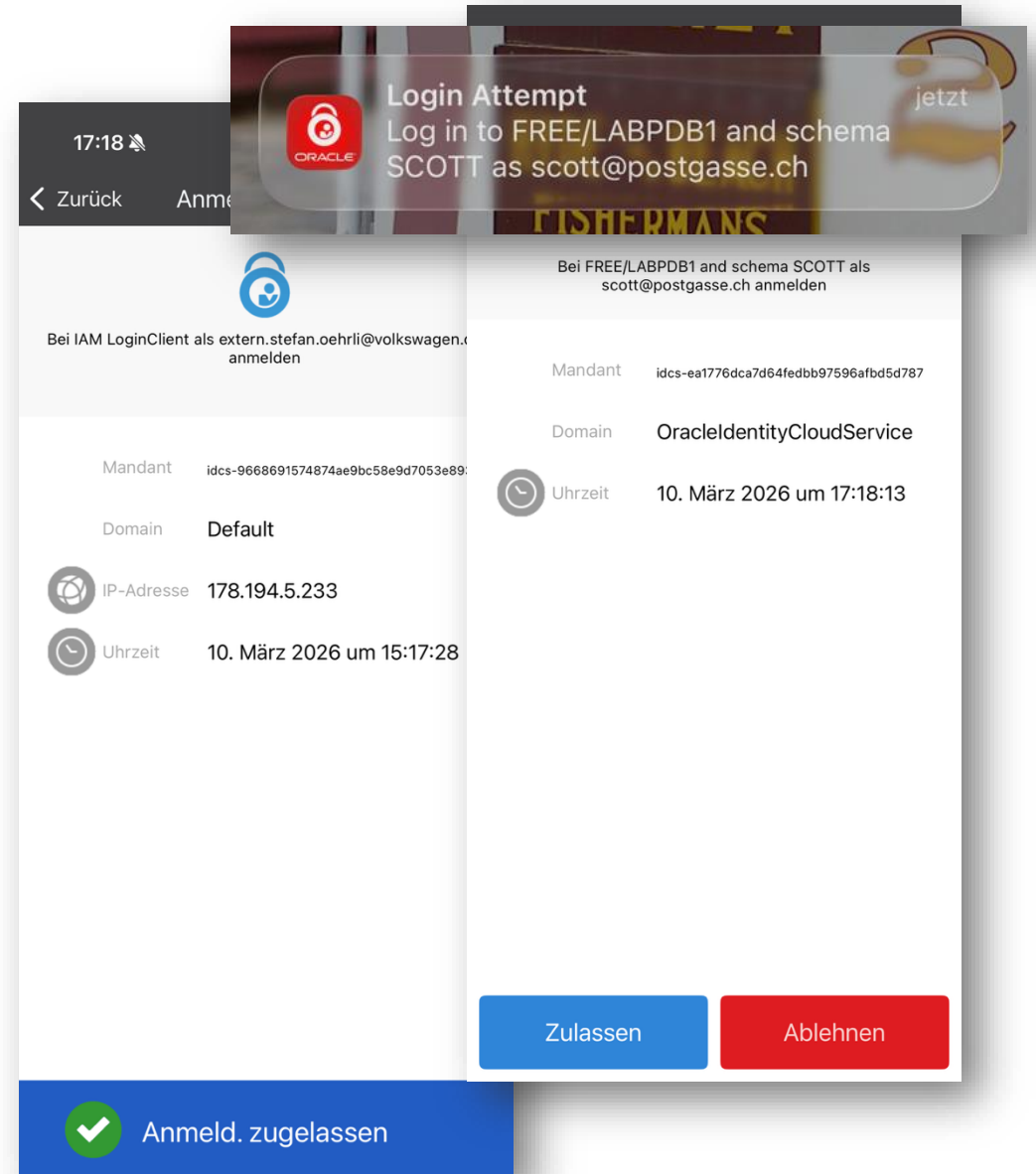


```
ALTER SYSTEM SET MFA_OMA_IAM_DOMAIN_URL = 'https://idcs...oraclecloud.com';
ALTER SYSTEM SET MFA_SMTP_HOST = 'smtp.email.eu-zurich-1.oci.oraclecloud.com';
ALTER SYSTEM SET MFA_SMTP_PORT = 587;
ALTER SYSTEM SET MFA_SENDER_EMAIL_ID = 'labdb.cdbfree@oradba.ch';
ALTER SYSTEM SET MFA_SENDER_EMAIL_DISPLAYNAME = 'LAB DB Admin';
```

Demo: Database Login with MFA

Authenticating with password and verification code

- Connect to the database client
- Enter database password
- MFA challenge appears
- Confirm the Login Request in Authenticator App
- Database session is established
- A few notes:
 - New column MFA in *dba_users*
 - New *USERENV* Variable
MULTIFACTOR_AUTHENTICATION_METHODS
 - Configuration based on DB, PDB Level => highly flexible



4

Authorization

Who can do what in the Database...

Authorization - Privileges

Simplified Operation and increased Security

Have you ever seen a database with **SELECT ANY** privileges?

- I.e. because someone needs access to the application schema
- Or tons of GRANT SELECT ON...

Oracle Database now does support schema privileges

- Grant access to a whole schema rather to individual objects

```
GRANT READ ANY TABLE ON SCHEMA SCOTT TO oehrli;
```

Introduction of new Views as part of this new privilege?

- DBA_SCHEMA_PRIVS, ROLE_SCHEMA_PRIVS, USER_SCHEMA_PRIVS, SESSION_SCHEMA_PRIVS, V\$ENABLEDSCHMAPRIVS

Authorization – READ Only

Allow restricted access to data

- Configure a user as **read only** user
 - override the privileges and roles that **have been** granted
 - allows `SELECT` operations but not `CREATE`, `INSERT`, `UPDATE`, or `DELETE`
- Create a read only user or alter

```
CREATE USER oehrli READ ONLY;
```

- Finding Information about read only user in ...
 - ...`DBA_USERS`

```
SELECT USERNAME, READ_ONLY from DBA_USERS  
WHERE USERNAME = 'OEHRLI';
```

- Granting **read only** access for maintenance or investigative reasons
- read-only access to parts of an application



Authorization – READ Only

Read-only access for local PDB users

- Test the READ only access as SCOTT

```
SQL> UPDATE emp SET sal=sal*1.2 WHERE ename='SCOTT';  
UPDATE emp SET sal=sal*1.2 WHERE ename='SCOTT'  
      *  
ERROR at line 1:  
  
ORA-28194: Can perform read operations only
```

Schema-Only Accounts

Secure database schemas without login capability

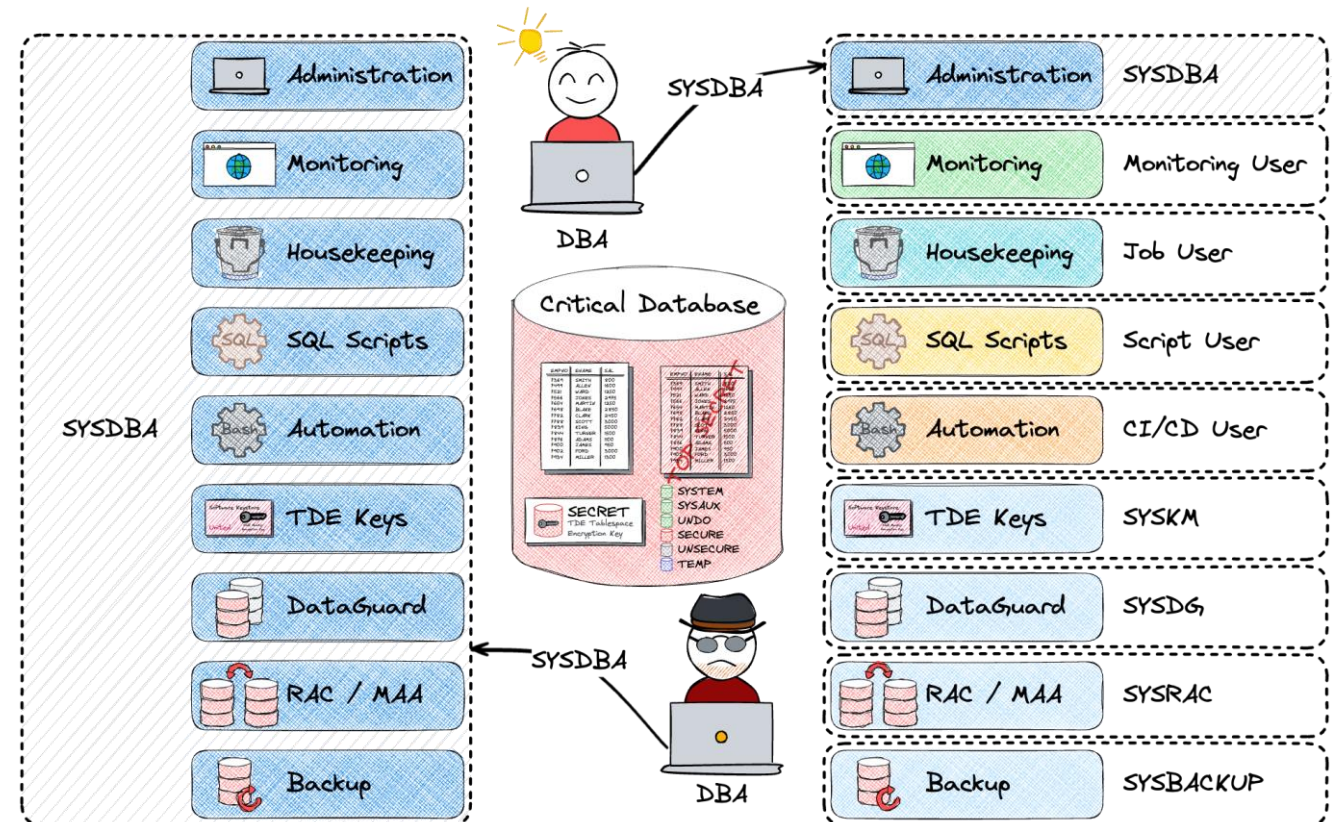
- Account owns database objects but **cannot log in**
- Created **without password or authentication method**
- Reduces attack surface for **application schemas**
- Common for **Oracle sample schemas (e.g. HR)**
- Recommended replacement for deprecated `PROXY_ONLY_CONNECT`

```
CREATE USER hr_app NO AUTHENTICATION;  
ALTER USER scott NO AUTHENTICATION;
```

Authorization – Developer Role

Simple role to start with application development

- New, ready-to-use role for developers e.g. necessary privileges for application development
- Previous **DBA role** - with many more rights than required for development
- Oracle will update the permissions in the role
- Highly recommended to implement the least privilege model
- Consider use of privilege analysis
 - E.g. dynamically identify used and unused privileges and roles.



Other Stuff

What else has been improved?

New database role for developers DB_DEVELOPER_ROLE

- **least-privilege** principles for application developer DBA role is not required
- **provides most of** the system and object privileges as well predefined roles, PL/SQL package privileges required for application development

Oracle Data Dictionary Protection

- Extended to **Non-SYS** Oracle schemas with separation of duties protection
- Other users cannot use system privileges e.g. ANY privileges) on the schema
- Can be enabled/disabled if required

```
SELECT username, dictionary_protected FROM dba_users  
WHERE dictionary_protected='YES';
```

5

Auditing

The DB is whatching
you...

Desupport of Traditional Auditing

Long announced and now finally implemented...

- Traditional Auditing not available any more
- Auditing as to be defined using audit policies
- Oracle Support Note [2909718.1](#) *Traditional to Unified Audit Syntax Converter - Generate Unified Audit Policies from Current Traditional Audit Configuration*
- Be carefull when upgrading Databases
 - Review your audit setting and concept

```
SQL> AUDIT CREATE TABLE;
```

```
AUDIT CREATE TABLE
```

```
*
```

```
ERROR at line 1:
```

```
ORA-46401: No new traditional AUDIT configuration is allowed. Traditional auditing is  
desupported, and you should use unified auditing in its place.
```

Oracle Default Audit Policies

Extension and supplementation of existing Oracle policies

Policy Name	Comment
ORA_SECURECONFIG	Audit policy containing audit options as per database security best practices
ORA_CIS_RECOMMENDATIONS	Audit policy containing audit options as per CIS recommendations
ORA_STIG_RECOMMENDATIONS	Audit policy to implement auditing recommendations from STIG v1 (4 Jan 2019)
ORA_ACCOUNT_MGMT	Audit policy containing audit options for auditing account management actions
ORA_DATABASE_PARAMETER	Audit policy containing audit options to audit changes in database parameters
ORA_LOGON_FAILURES	Audit policy containing audit options to capture logon failures
ORA_ALL_TOPLEVEL_ACTIONS	Audit policy to track all top level actions to help comply with STIG v1 (4 Jan 2019). It should be enabled only on privileged users;
ORA_LOGON_LOGOFF	Audit policy to track session logon and logoff actions to help comply with STIG v1 (4 Jan 2019) and CIS V2.0.0 (12-28-2016) It should be enabled only on privileged users;
ORA\$DICTIONARY_SENS_COL_ACCESS	Audit policy to audit access to dictionary sensitive columns (01 Jun 2022)

- Consider using *AUDIT_UNIFIED_POLICY_COMMENTS* for your own policies
- Bug 32694238: unified_audit_policies column should clearly indicate mandatory audit records



Audit Use Cases

It is time to define / implement a decent audit concept



Other Audit Enhancements

Small but helpful improvements...

- Column Level Audit for Tables and Views
 - Allow to specify a column for action UPDATE
 - Create more granular and focused audit policies
 - Does not make audit concept easier 😊

```
CREATE AUDIT POLICY scott_sal ACTIONS UPDATE (sal) ON scott.emp;
```

- Behaviour change for AUDIT POLICY statement
 - Changes made to the audit policy become effective **immediately...**
 - ...in the current session
 - ...in all active sessions without re-login
 - Audit deployment is therefore **much** easier => no downtime

Just one more thing...

It seems that there are new functions in the queue.

- New hidden parameter related to audit

```
SQL> @hip prote%audit
```

Parameter	Session Instance	S	I	D	Description
-----	-----	-	-	-	-----
_enable_protected_audit_policy	FALSE				Allow Protected Unified Audit Policy Enforcement

- Along with a new undocumented column in AUDIT_UNIFIED_POLICIES

```
SQL> desc AUDIT_UNIFIED_POLICIES
```

Name	Null?	Type
-----	-----	-----
POLICY_NAME		VARCHAR2 (128)
...		
ORACLE_SUPPLIED		VARCHAR2 (3)
PROTECTED		VARCHAR2 (3)
COLUMN_NAME		VARCHAR2 (128)

- Possibility to enforce audit policies in PDBs



6

Encryption

At REST and in transition

Encryption at REST

Changes around Transparent Data Encryption (TDE)

Encryption **Algorithm** changes

- The default encryption algorithm for TDE Column and Tablespace is now **AES256**
- Decryption libraries for the GOST and SEED are desupported

Changed Encryption **Modes**

- **TDE Column** Galois/Counter mode (GCM) instead of Cipher Block Chaining (CBC),
- **TDE Tablespace** Tweakable Block Ciphertext Stealing (XTS) operating mode or cipher feedback (CFB) whereby XTS is the default mode.

```
CREATE TABLESPACE users_enc DATAFILE  
' /u02/oradata/CDB23A/users_enc01CDB23A.dbf' SIZE 100M  
ENCRYPTION USING AES256 MODE 'XTS' ENCRYPT;
```

Encryption at REST

Changes around Transparent Data Encryption (TDE)

Broader use of **SHA256**

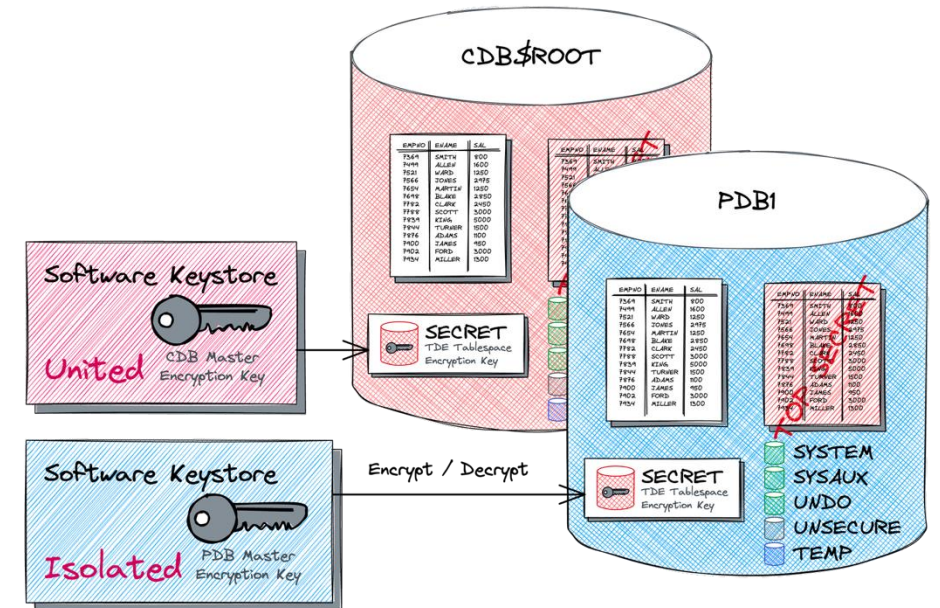
- Oracle Recovery Manager (Oracle RMAN) integrity check now uses SHA512
- Oracle RMAN and column keys are now derived from SHA512/AES for key generation

Improved Local **Auto-Login** Wallets

- Wallet is now more tightly bound to the host
- Support both bare metal and virtual environments
- Mmh, so in the past this was not so good in this case?

New parameter to Control the TDE Rekey Operations

- **DB_RECOVERY_AUTO_REKEY** controls whether an Oracle Data Guard standby database recovery operation



Encryption in Transition

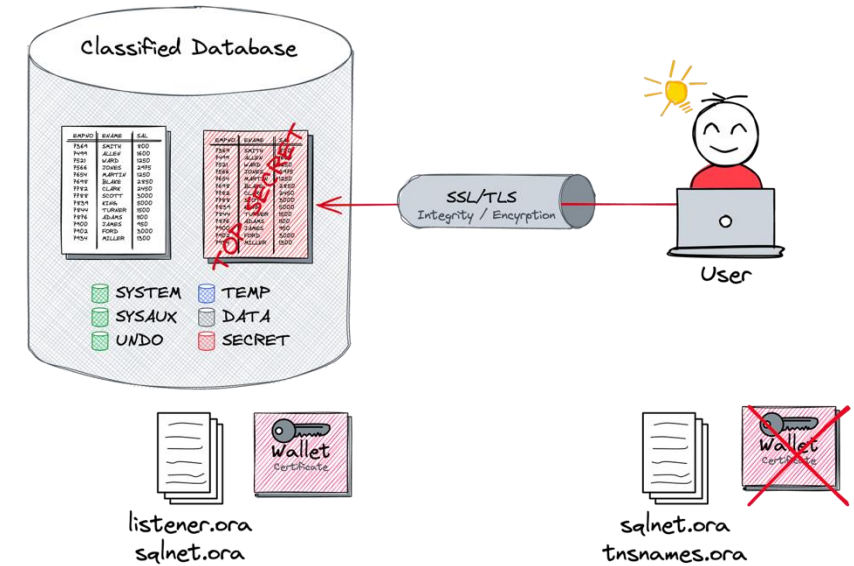
Changes related to Network Encryption, Certificates, TLS

TLS 1.3 finally arrived in Oracle AI Database

- Oracle AI Database 26ai Transport Layer Security (TLS) version 1.3
- Initial session setup more efficiently than earlier TLS versions
- Configure in *sqlnet.ora* using `SSL_VERSION` and `SSL_CIPHER_SUITES`

Simplified Transport Layer Security Configuration

- Ability to Configure Transport Layer Security Connections **without Client Wallets**
- `SSL_VERSION` parameter does accept a comma-separated list e.g. TLSv1.3, TLSv1.2
- Introduction of the `ALLOWED_WEAK_CERT_ALGORITHMS` parameter
- Modifications to how wallets are loaded
 - **Server-side wallets** `WALLET_LOCATION` deprecated use `WALLET_ROOT` from *init.ora*
 - **Client-side wallets** Still use `WALLET_LOCATION` parameter, now defaults to `TNS_ADMIN`



7

Further Innovations

What else?

Further Innovations

What else...

A bunch of new SQLNet Parameter to control **weak, deprecated** ciphers

- e.g. SSL_ALLOW_WEAK_DN_MATCH

Azure Active Directory Integration

- Autonomous Database now can accept Azure AD **OAuth2** tokens to access the database

Authenticating and Authorizing IAM Users for Autonomous Database on dedicated Exadata

- **Enhanced Connection** Options:
 - Applications connect using end-user, instance, and resource principals.
- **Proxy Capabilities** for IAM Users:
 - IAM users can proxy via database user schema.
- **Database Link** Support:
 - IAM connections now support database links.



Database Security Assessment Tool (DBSat)

Latest Release Ready for Oracle 26ai – Version 4.2.0 February 2026

STIG 19c V1R1 compliance

- includes 30 new STIG findings and revised STIG group IDs

Enhanced Auditing and Security

- New auditing results, overall, up to 120 Security checks
- Support for Oracle AI Database 26ai SQL Firewall

Sensitive Data Discovery

- Indian PAN and Aadhaar numbers

Improved Clarity and Quality

- one-line summary outline
- Compliance labels

Operational Enhancements

- New parameter
- Linux 64-bit ARM Support

The screenshot displays the 'Patch Check' tool interface. It features a header with 'INFO.PATCH' and a status bar with 'CIS', 'OBP', and 'STIG' labels. The main content area is divided into sections: 'Status' (High Risk), 'Summary' (Oracle Database version is supported but latest patch is missing), 'Details' (Latest patch not applied for a supported database version.), 'Remarks' (Unsupported commercial and database systems should not be used because fixes to newly identified bugs will not be implemented by the vendor...), and 'References' (Oracle Best Practice, CIS Benchmark: Recommendation 1.1, DISA STIG: V-237697, V-237748, V-251802). Annotations include: 'Rule ID' pointing to 'INFO.PATCH'; 'Brief description of recommended Action' pointing to the summary; 'Comprehensive breakdown of the finding' pointing to the details; 'Rationale and Recommendations' pointing to the remarks; 'Mapping to Regulations' pointing to the references; and 'Label Indicating Relevance to Regulations' pointing to the 'STIG' label. A red line connects the 'High Risk' status to the 'Possible Risk Levels: Evaluate, Advisory, Low, Medium, or High' text.

Rule ID

Brief description of recommended Action

Comprehensive breakdown of the finding

Rationale and Recommendations

Mapping to Regulations

Label Indicating Relevance to Regulations

Possible Risk Levels: Evaluate, Advisory, Low, Medium, or High

Patch Check	
INFO.PATCH	The Oracle Database should be patched
Status	High Risk
Summary	Oracle Database version is supported but latest patch is missing. Latest comprehensive patch has not been applied.
Details	Latest patch not applied for a supported database version.
Remarks	Unsupported commercial and database systems should not be used because fixes to newly identified bugs will not be implemented by the vendor. The lack of support can result in potential vulnerabilities. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities, which leaves them subject to exploitation. When maintenance updates and patches are no longer available, the database software is no longer considered supported and should be upgraded or decommissioned.
References	It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates on a regular quarterly schedule. These updates should be applied as soon as they are available. Oracle Best Practice CIS Benchmark: Recommendation 1.1 DISA STIG: V-237697, V-237748, V-251802

Why Oracle Data Safe?

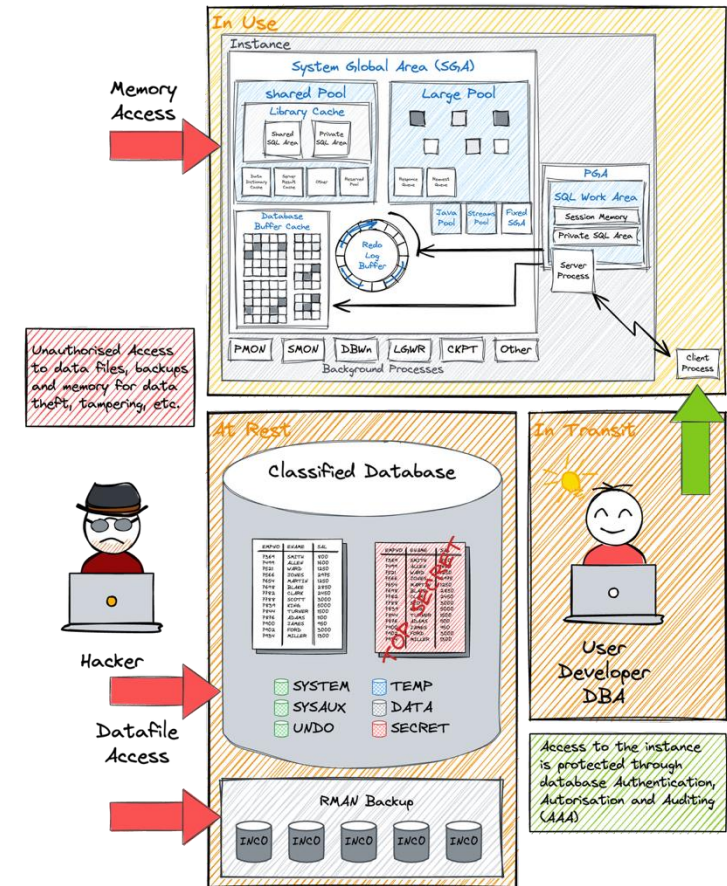
Beyond Encryption and Patching – Comprehensive Database Security

More Than Basic Security – Encryption and patching are crucial but incomplete.

Key Security Focus Areas:

- **Configuration Compliance** – Is the database securely configured?
- **User Risk & Monitoring** – Who are the highest-risk users, and what actions are they performing?
- **Audit & Compliance** – Which activities should be audited, and how do we manage and protect the audit logs effectively?
- **Sensitive Data Control** – What sensitive data is stored, and can exposure be minimized?

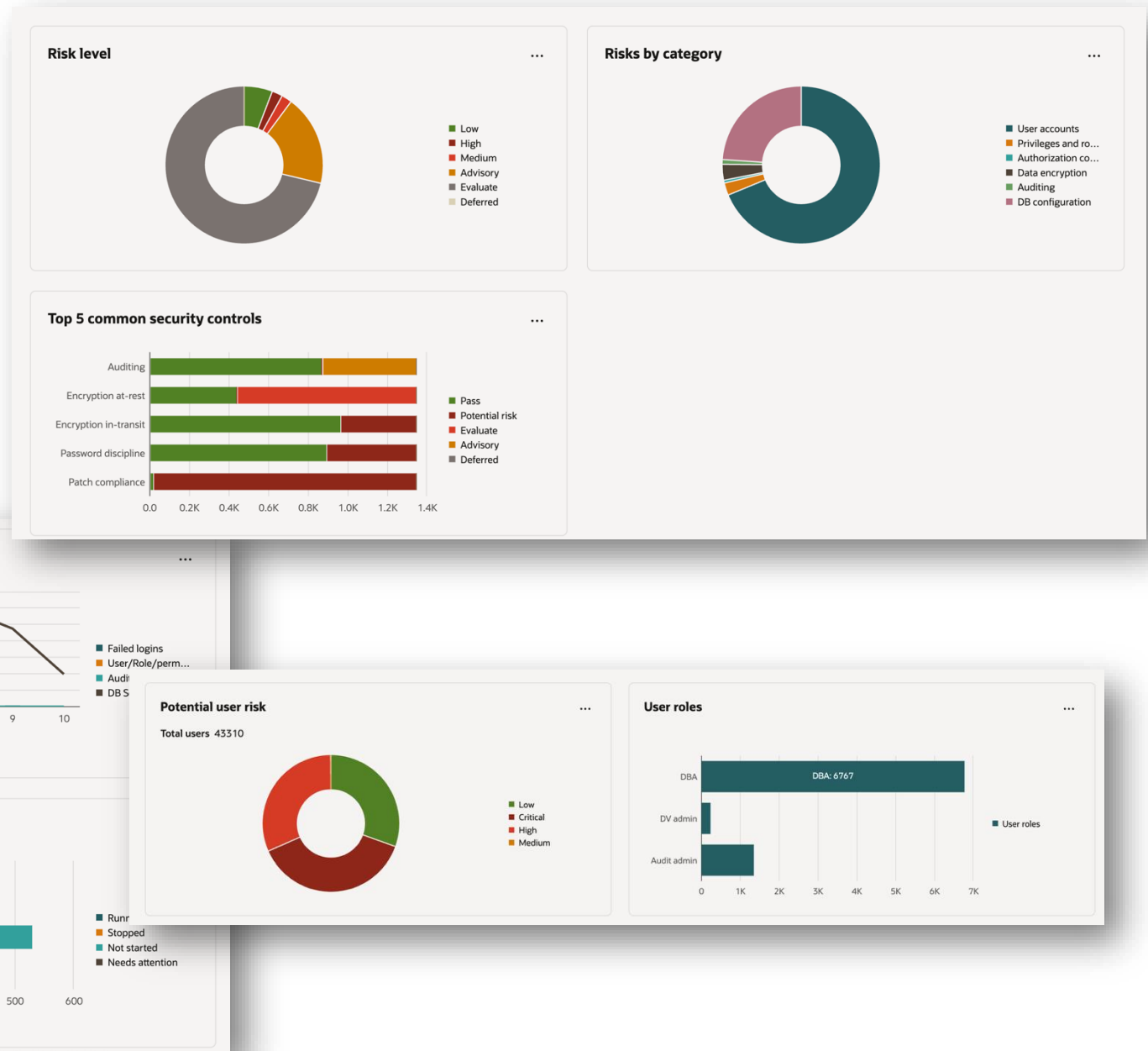
***Holistic Security Management** – Oracle Data Safe offers centralized tools to address these areas, enhancing control, visibility, and compliance.*



Data Safe Dashboard

Key Security Indicators at a Glance

- Security Assessment Overview
- User Assessment Overview
- Activity Auditing Overview



Securing Data Access in the AI Era

New approaches to enforce user-level data boundaries

- AI agents may operate with **broader database privileges**
- Risk: users access **more data via AI** than they are normally allowed
- Need to enforce **user-level data boundaries** inside the database
- Combines concepts similar to **VPD, Database Vault, and other controls**
- Goal: each user effectively sees **only their permitted data**
- **Currently under development**

Simplifying Database Security

Fewer Complex Queries, More Actionable Insights

What if...

- You could instantly know the security status of your database?
- Get insights into unusual or risky activity inside your DB?
- Simplify the work of a security operator or analyst?
- All this could be achieved without the need for complex SQL queries or in-depth technical know-how?

A Preview

- A future feature currently in highly alpha state
- Still uncertain on final capabilities and release dates
- All information subject to change



Data Safe – Security Advisory

Preview of Future Data Safe Feature – Highly Experimental, Subject to Change

The screenshot displays the Oracle Cloud Security Advisor interface. The top navigation bar includes the Oracle Cloud logo, a search bar, and the region 'US East (Ashburn)'. The breadcrumb trail shows 'Data Safe > Security center > Security advisor'. The left sidebar lists various security features: Security advisor (selected), Dashboard, Security assessment, User assessment, Data discovery, Data masking, Activity auditing, SQL Firewall, and Alerts. Below this is the 'Session scope' section with a dropdown menu showing 'adscorp_tenant01 (root)'. The main content area is titled 'Security advisor' and features a search bar with the query 'What has ALEX_APPMGR done recently? Include database, sql text, and time of activity'. The results show activity for 'ALEX_APPMGR's Recent Activity' on 'Sep 2, 2024, 11:28 PM' and 'Sep 2, 2024, 11:23 PM'. The activity is categorized by database: 'HR_PRODUCTION Database' and 'HR_DEVELOPMENT Database'. Each category lists several SQL queries. A link to 'Activity Auditing' is provided for further details. At the bottom, there is a text input field for asking questions, a 'Send' button, and a 'History' button. A disclaimer at the very bottom states: 'Disclaimer: The Data Safe assistant relies on artificial intelligence models or systems. While helpful when properly used, materials generated may be incomplete and/or contain errors and inaccuracies. Your access and use of this feature is at your own risk. Oracle has no responsibility or liability for any damages resulting from such access or use.'

ORACLE Cloud Search resources, services, documentation, and Marketplace US East (Ashburn)

Data Safe > Security center > Security advisor

Security center

Security advisor

Dashboard

Security assessment

User assessment

Data discovery

Data masking

Activity auditing

SQL Firewall

Alerts

Session scope

Compartment

adscorp_tenant01 (root)

What has ALEX_APPMGR done recently? Include database, sql text, and time of activity

Fri, 06 Sep 2024 02:39:23 UTC

ALEX_APPMGR's Recent Activity:

Here's a summary of ALEX_APPMGR's recent activities across the HR_PRODUCTION and HR_DEVELOPMENT databases:

HR_PRODUCTION Database:

- Sep 2, 2024, 11:28 PM:
 - SELECT last_name, salary from hcm.employees
 - SELECT first_name, last_name, email from hcm.employees
 - SELECT street_address, city from hcm.locations
 - SELECT job_title, max_salary from hcm.jobs

HR_DEVELOPMENT Database:

- Sep 2, 2024, 11:23 PM:
 - SELECT first_name, last_name, email from hcm.employees
 - SELECT last_name, salary from hcm.employees
 - SELECT street_address, city from hcm.locations
 - SELECT job_title, max_salary from hcm.jobs

You can review further details and the full audit trail for this user via Data Safe's Activity Auditing feature: [Activity Auditing](#)

Please ask your question here...

Send

History

Disclaimer: The Data Safe assistant relies on artificial intelligence models or systems. While helpful when properly used, materials generated may be incomplete and/or contain errors and inaccuracies. Your access and use of this feature is at your own risk. Oracle has no responsibility or liability for any damages resulting from such access or use.

Conclusion

Database Security with Oracle 26ai: Not Just a Simple Maintenance Update

SQL Firewall: A Major Milestone

- The SQL Firewall stands out as a pivotal feature in Oracle 26ai

Continuous Enhancement, Not Just Maintenance

- Impactful improvements beyond routine updates
- Enhancements integral to ongoing security evolution

Assessing with the Latest Tools

- Utilize latest DB Sat for 26ai security assessment
- Advanced tool alignment with Oracle 26ai capabilities

Personal Favorite Immediate Audit Policy Implementation

- Simplifies and enhances audit processes

Security checklist

Anti-SQL-injection protection



SSL and OpenSSL up to date



Passwords hashed with salt



Multi-factor authentication on the back-office



AES encryption on sensitive data



Preventing the PM from sending the whole unencrypted database by email



CommitStrip.com



**Oracle 26ai new security
features demand a strategic
approach to unlock their full
potential**

Oracle LiveLabs

Test the functions of the Oracle AI Database without having to worry about setting up the infrastructure.

The screenshot shows the Oracle LiveLabs website interface. At the top, there's a navigation bar with the LiveLabs logo, a search bar containing 'Database Security', and links for 'Event Code' and 'Sign In'. Below the navigation bar, the main content area is titled 'Workshops and Sprints'. On the left side, there's a sidebar with filters. The 'Sort By' dropdown is set to 'Most Popular'. The 'Number of Workshops' is 42. The 'Level' filter shows 'Beginner (20)', 'Intermediate (20)', and 'Advanced (2)'. The 'Workshop Type' filter shows 'Paid Credits (36)', 'Run on LiveLabs (21)', 'Sprints (5)', 'Run on Gov Cloud', and 'ADB for Free'. The 'Workshop Series' filter shows 'Database Security Series (15)'. The main grid displays six workshops, each with a database icon, title, description, duration, and view count. A red Oracle logo is visible in the bottom right corner of the grid.

Workshop Title	Duration	Views
DB Security - Audit Vault and DB Firewall	2 hrs, 30 mins	60722 Views
DB Security - ASO (Transparent Data Encryption & Data Redaction)	1 hr	44586 Views
DB Security - Key Vault	1 hr	42133 Views
DB Security - Data Masking and Subsetting on Enterprise Manager 24ai	1 hr, 30 mins	28864 Views
DB Security - Database Security Assessment Tool (DBSAT)	2 hrs	24064 Views
DB Security - Database Vault	1 hr	22708 Views

<http://livelabs.oracle.com>

Oracle Cloud

Create you own Autonomous Database 26ai => Developer Edition

cloud.oracle.com/db/adbs/adv/create?region=eu-zurich-1

Cloud Search resources, services, documentation, and Marketplace Switzerland North (Zurich)

Create Autonomous Database Serverless

Run Autonomous Database on serverless architecture. [Learn more.](#)

Display name
adb-zrh-lab-lab-00-atp23ai
A user-friendly name to help you easily identify the resource.

Database name
LAB00ATP23AI01
The name must contain only letters and numbers, starting with a letter. Maximum of 30 characters.

Compartment
OCI-Lab
oradbbaace (root)/OCI-Lab

Workload type

Data Warehouse
Built for decision support and data warehouse workloads. Fast queries over large volumes of data.

Transaction Processing
Built for transactional workloads. High concurrency for short-running queries and transactions. ✓

JSON
Built for JSON-centric application development. Developer-friendly document APIs and native JSON storage.

APEX
Built for Oracle APEX application development. Creation and deployment of low-code applications, with database included.

Database configuration

Always Free 

Developer 

Choose database version
23ai

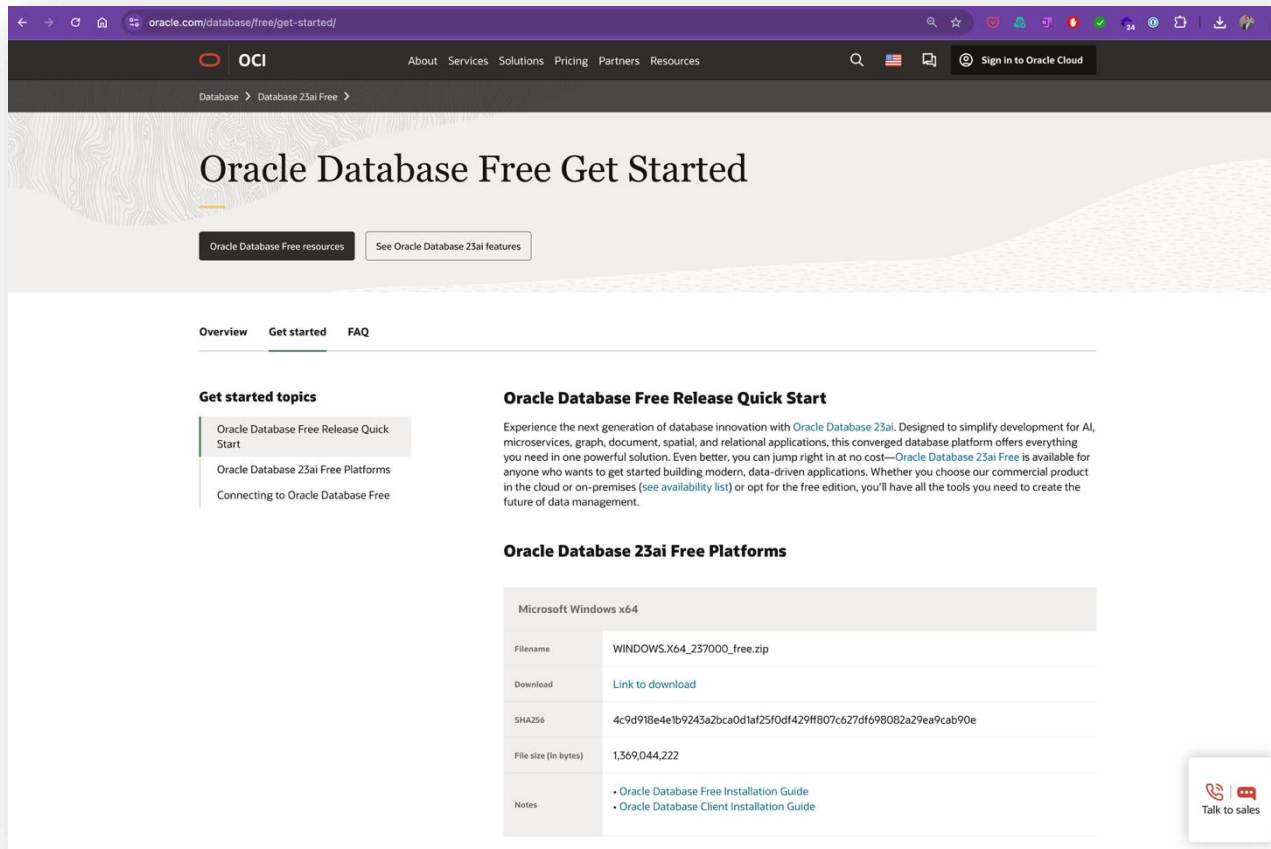
[Show advanced options](#)

Create Save as stack Cancel

Terms of Use and Privacy Cookie Preferences Copyright © 2025, Oracle and/or its affiliates. All rights reserved. What's this? | Redwood preview 

Oracle 26ai locally

Either setup Oracle 26ai yourself or use a precreated VM or container



RPM package available for Platforms / OS

- Oracle Linux / Enterprise Linux 8 x86_64
- Oracle Linux / Enterprise Linux 9 x86_64
- Oracle Linux 8 arm / aarch64
- Microsoft Windows x64

Pre-Configured Installations

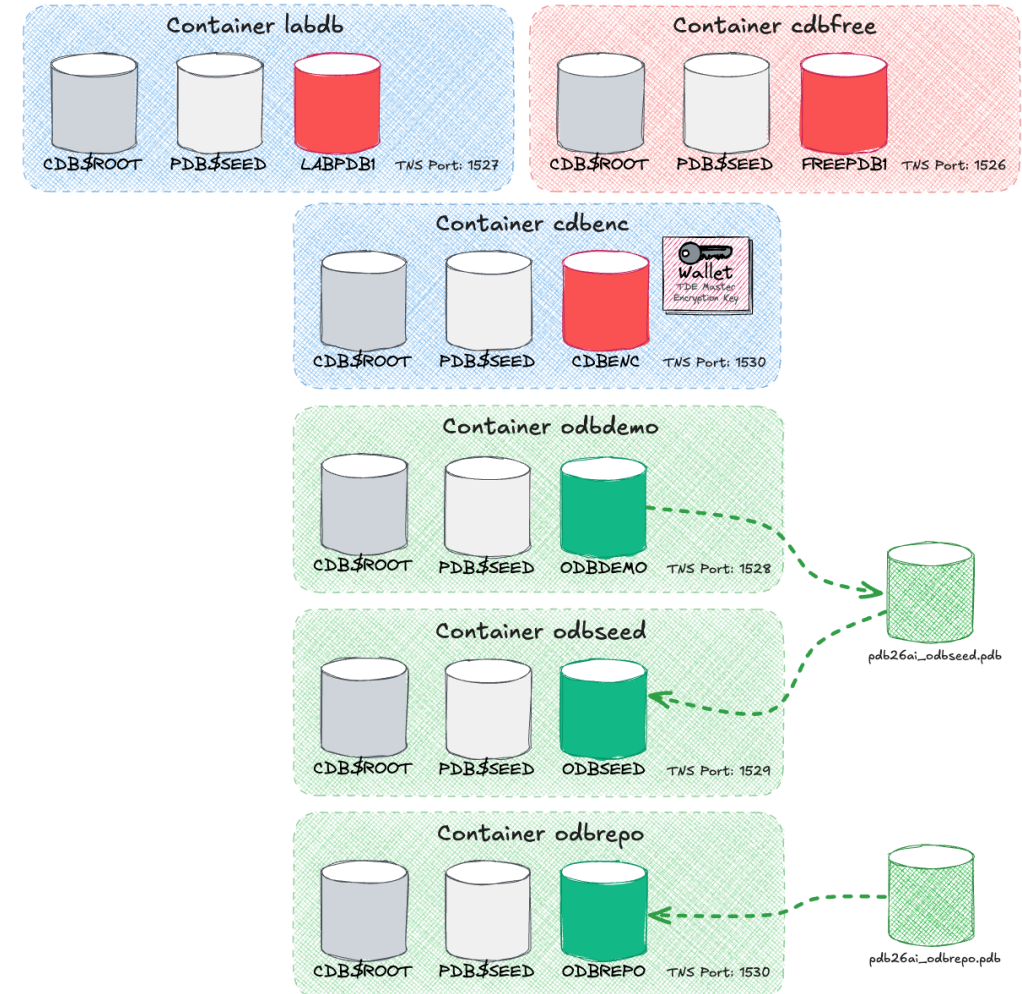
- Docker / Podman
<https://container-registry.oracle.com/>
- Oracle Virtualbox
https://download.oracle.com/otn_software/virtualbox/dd/Oracle_Database_26ai_Free_Developer.ova

Local Oracle Security Lab in Minutes

Oracle AI Database 26ai Free – Reproducible Container Lab Environment

- Container-based lab using **Docker or Podman**
- Runs **Oracle AI Database 26ai Free** locally
- Multiple ready-to-use scenarios (test DB, security lab, demo environments)
- **Preconfigured scripts and PDB archives** for fast setup
- **Reproducible environments** – reset, clone, or rebuild easily
- Ideal for **testing security features, demos, and training**

<https://github.com/oehrlis/oracle-free-labs/tree/main>



Thank You

