Oracle Unified Audit

You have started with Unified Audit? But what happens next?

August 2023

Stefan Oehrli

Stefan Oehrli – Data Platforms

Oracle ACE Pro

stefan.oehrli@accenture.com

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

>

DATA PLATFORMS

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints, assets and tools.

3 key benefits

1 Architecture expertise from hands-on projects

2 Delivery of tailor-made data platforms

3 Integrated Teams - Like a Rowing team, perfect alignment and interaction.

Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project’s needs.

Expertise

Expert group for modern data platforms from technical implementation to project management and organization

Oracle Audit

What must be considered when configuring Oracle Database Audit?

1 Introduction

2 Conceptual Considerations

3 Good Practice

4 Reporting and Analysis

5 Special Use Cases

6 Migration

7 Central Audit Management

8 Conclusion

1

Introduction

Why is Oracle Database Audit needed at all?

Introduction

Motivation for Oracle Database Audit

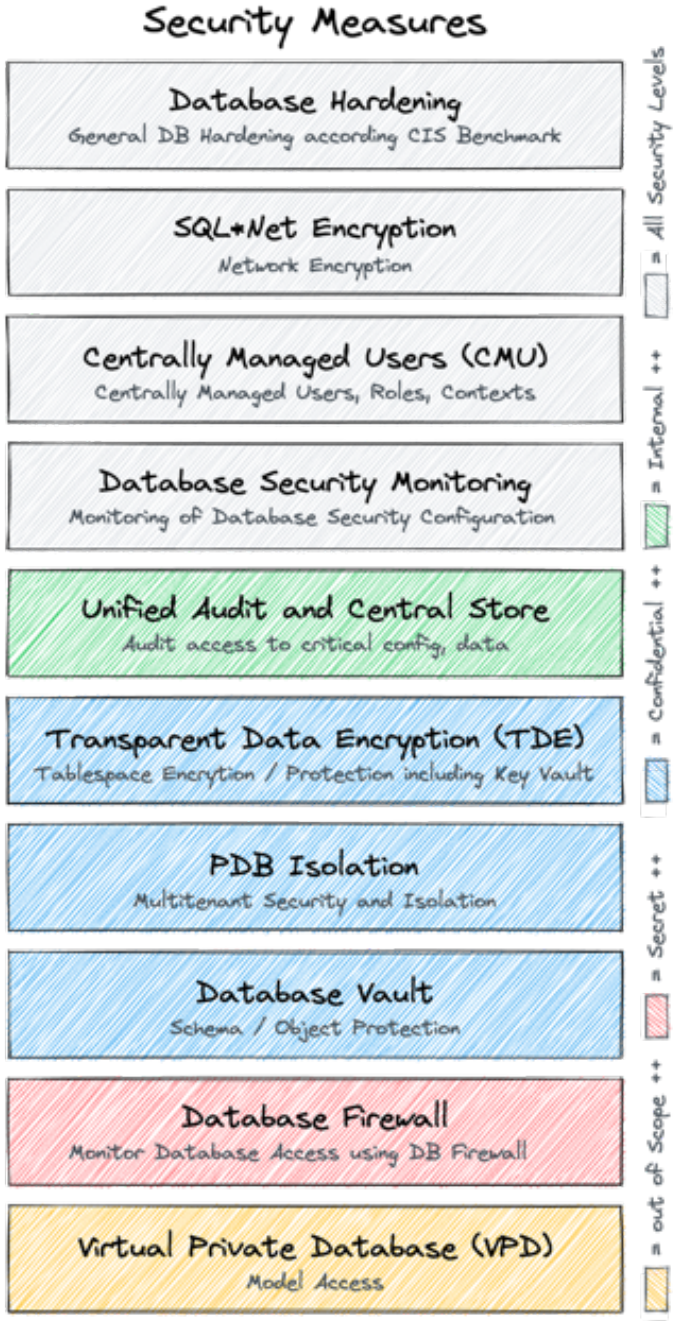
Why Database Security at all?

- Protection of **company** and its business
- Protection of **employees**, **customers** and others
- and of course, **compliance** and **regulatory** requirements

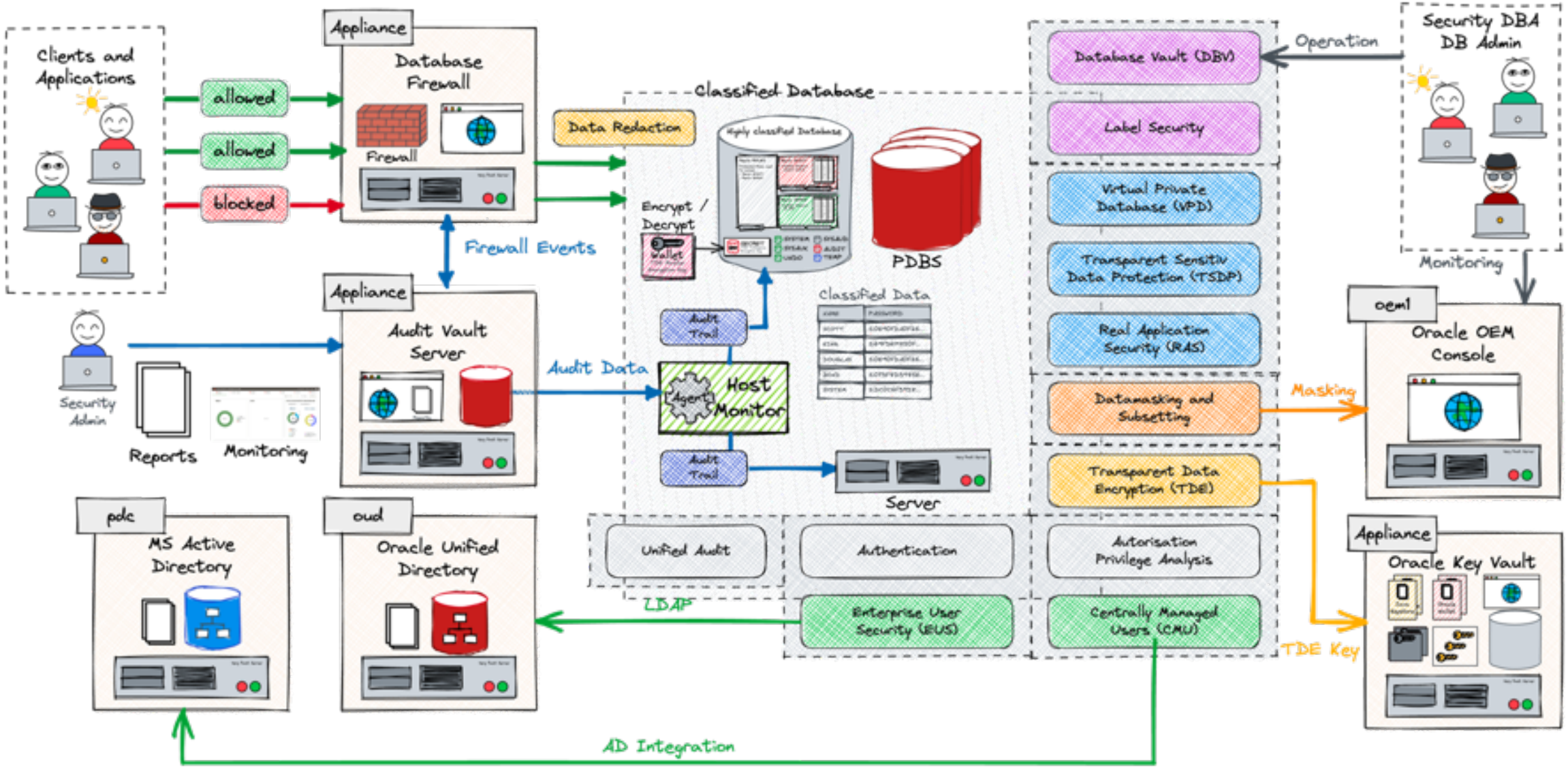
Security measures are complex and expensive

- **Management** of security configuration e.g., Audit
- Availability of **Security Options** and **Features** (Edition, License etc.)
- **Segregation of Duties** e.g., DBAs audit themselves?
- Traceability and auditability

Oracle Audit Vault and Database Firewall as Audit warehouse, Audit management and security measure enforcement tool



Maximal Data Security Architecture



2

Conceptual Considerations

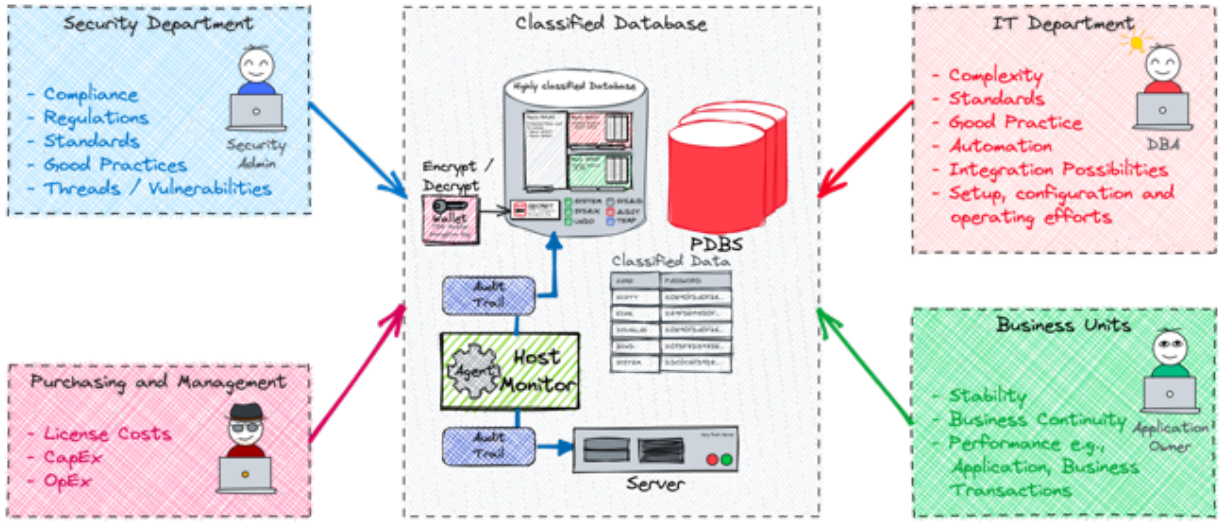
What to consider when starting Database Audit

A few basic Requirements

What do you need to consider before starting with database audit?

What is the objective?

- Simple audit because it is part of it?
- Internal Security Standards / Requirements?
- Regulatory and Compliance requirements with clear specifications?
- Is there a specific Use Case to be covered?
- Distinction between Application Audit and Database Audit



Further important Considerations

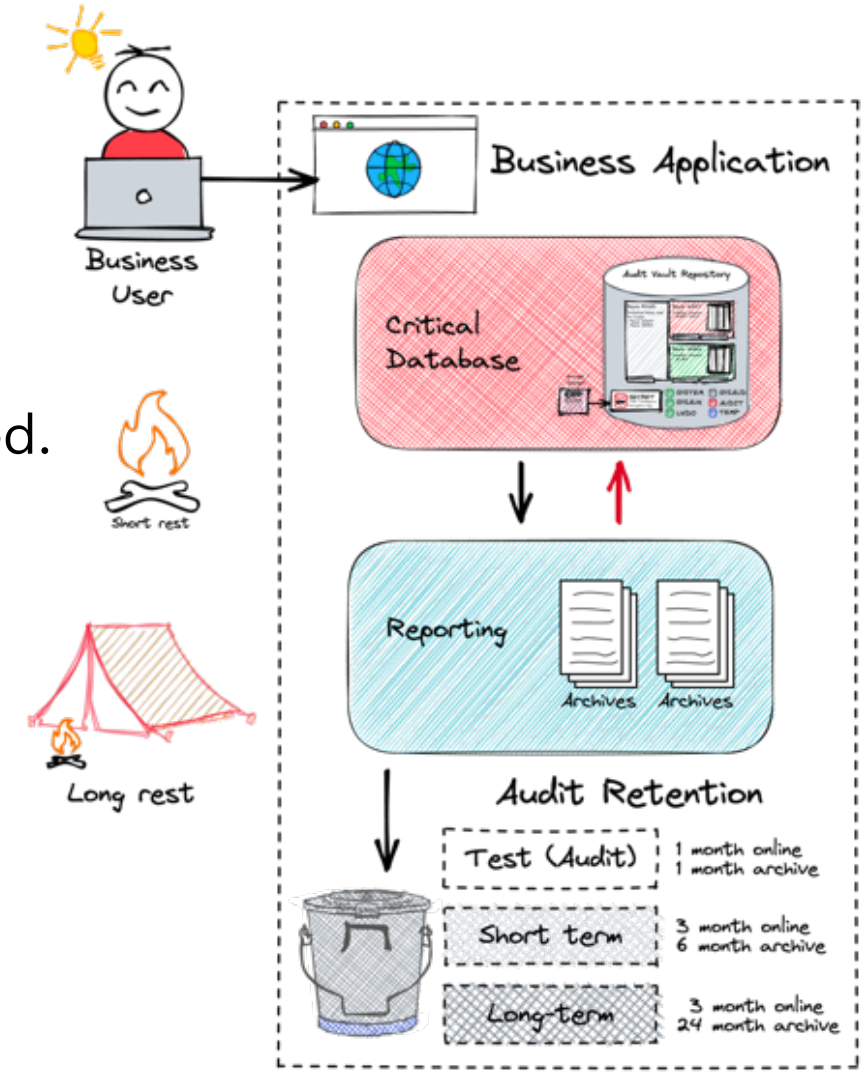
Questions that need to be clarified before using the database Audit

How will the Audit data **be analysed**?

- Risk of creating a Data Graveyard if not defined
- Trade-offs between what is necessary, possible and desired.
- Consider Legal Requirements

How Long should Audit Data be available?

- Retention time defines Storage requirement
- Main drivers of operating and resource costs
- Consider different levels of aggregation of audit data



Default Policies and Best Practice

Which Audit Policies are useful?

Oracle offers convenient **standard Audit Policies**

- Not enabled by default
- Change them between the major versions or improved in release updates
- Covering basic Audit Use Cases e.g.,
  - Account Management ORA_ACCOUNT_MGMT
  - CIS Recommendations ORA_CIS_RECOMMENDATIONS

```
SELECT policy_name FROM audit_unified_policies
WHERE oracle_supplied='YES' GROUP BY policy_name;
```

Consider the White Paper Oracle Database Unified Audit - Best Practice Guidelines

- Provides detailed information for Audit Policies and different Use Cases
- Does cover Audit policies for a plain Database, *Oracle Data Safe* as well *Oracle AVDF*

Audit Use Cases

What kind of Audit Events should be covered?

Audit Use Cases

Which policies should be enabled?

3

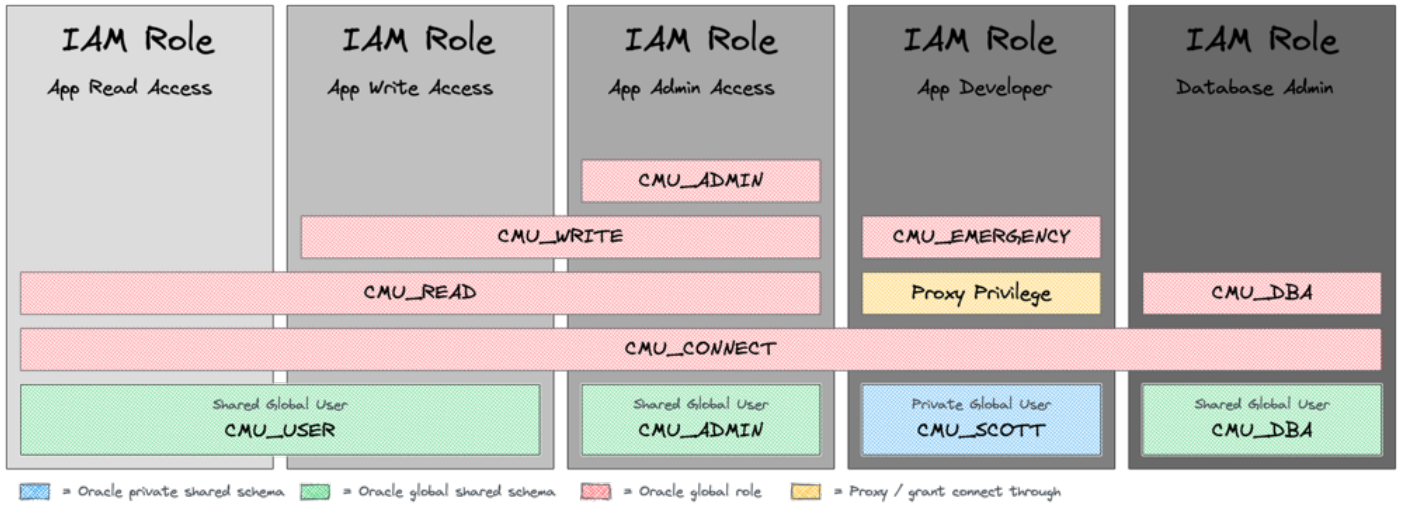
Good Practice

What has worked well for Unified Audit?

User and Role Concept

Without a concept, you have no idea who should be audited and how

- Definition of **distinguished** user Groups and Roles
- Implementation of the Principle of **Least Privilege**
  - Use tools like privilege capture to analyse
- Do not use SYSDBA / DBA for “everything”
  - Appropriate use of SYSDG, SYSKM, etc.



Retention

Where should what be stored and for how long...?

Local storage of raw Audit Data

- Only as long as necessary
- Relatively high resource and operating Costs

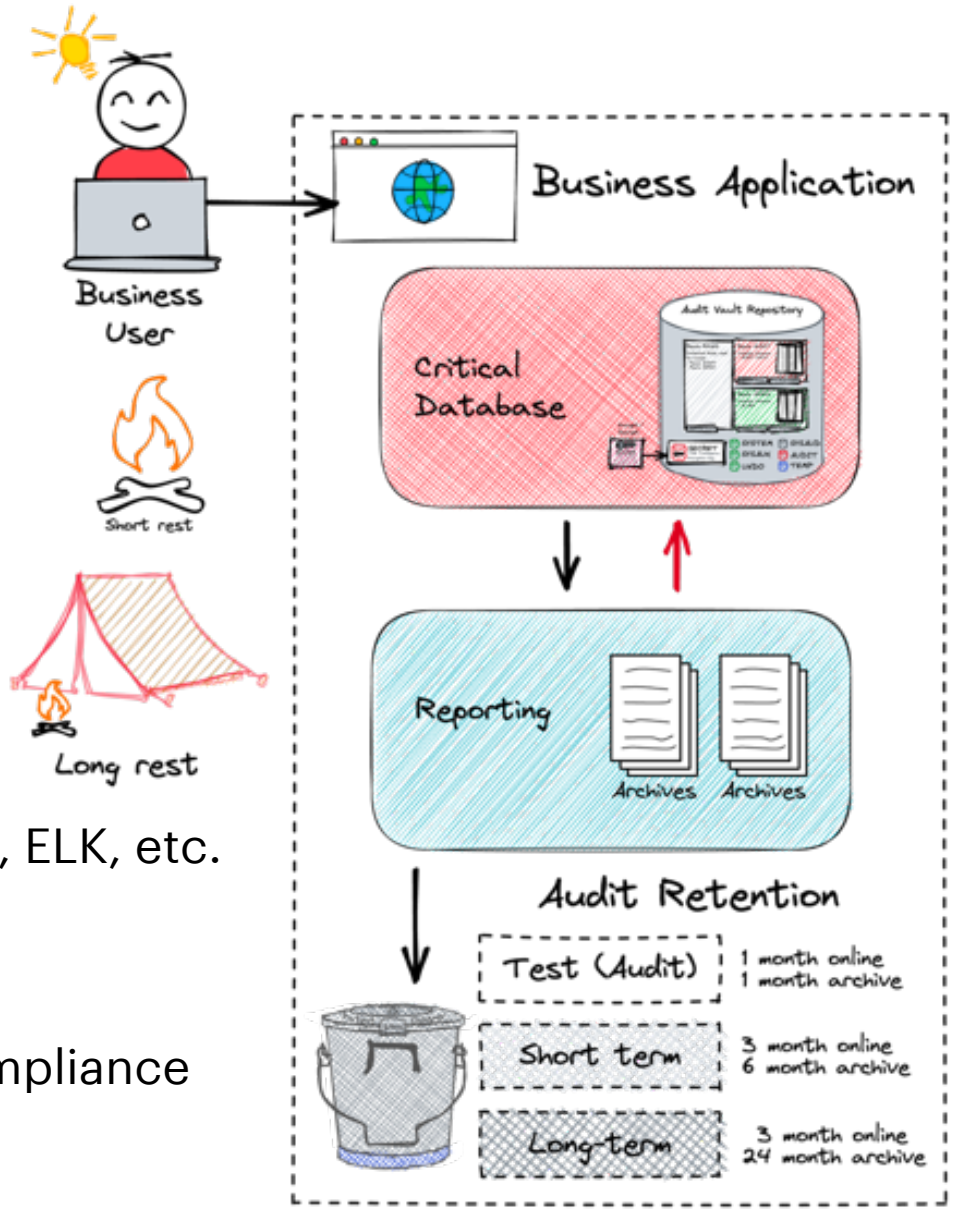
Central storage of raw Audit Data

- Lower Costs and Availability
- Oracle-based or third-party Solution e.g., Oracle AVDF, Splunk, ELK, etc.

Long-term storage of aggregated Data / Reports

- Only the mandatory / required reports for the fulfilment of Compliance requirements

Consider **central storage** and **automatic housekeeping** of Audit Data



Housekeeping

Rolling window of available Audit Data

- Daily DBMS_SCHEDULER Job to set the Audit Archive Timestamp for SYSDATE-Retention

```
DBMS_SCHEDULER.CREATE_JOB (
  job_name   => 'DAILY_UNIFIED_AUDIT_TIMESTAMP',
  job_type   => 'PLSQL_BLOCK',
  job_action => 'BEGIN DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(AUDIT_TRAIL_TYPE =>
       DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,LAST_ARCHIVE_TIME => sysdate-&retention); END;',
  start_date => sysdate,repeat_interval => 'FREQ=HOURLY;INTERVAL=24', enabled => TRUE,
  comments   => 'Archive timestamp for unified audit to sysdate-&retention');
```

- Daily job defined to purge everyhing older than last archive timestamp

```
DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
  audit_trail_type            => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
  audit_trail_purge_interval  => 24 /* hours */,
  audit_trail_purge_name      => 'Daily_Unified_Audit_Purge_Job',
use_last_arch_timestamp       => TRUE);
```

Further Measures

Proven methods based on practical experience…

Dedicated Tablespace for Audit Data

- Create a separate tablespace for Audit Trail and move it with *DBMS_AUDIT_MGMT*

Optimize the **Partition Internval** for your Audit Data Retention

- Default Interval set to 1 month consider a lower e.g., 1 day if you purge data daily

Create **multiple** Audit Policies

- Do not create a *"one Audit Policy fit's all"* => Define **manageable Use Cases** and corresponding Audit Policies e.g., with conditions, for User, Roles etc.
- Overlapping Audit Policies do not double the Audit Data

Define **dedicated** Audit **Admin** and **Reporting** Users

5

Reporting and Analysis

Simple and straight forward analysis of the audit data

SQL*Plus Reporting

Let's dive into Audit Reporting via Command Line

- A series of simple but useful reports

What kind of reports are available?

- **Audit Configuration** info about policies, storage and jobs
- **Audit Sessions** reports to analyse audit sessions
- **Generate Statements** scripts to generate statements to enable, disable, drop and create policies
- **Top Audit Events** a couple of top audit event reports e.g. by user, policy, action and more

Where to find?

- Available via GitHub Repository oehrlis/oradba
- Blog post SQL Toolbox for simplified Oracle Unified Audit Data Analysis

SQL Developer Reporting

Let's dive into the slightly more pleasant Audit Reporting

- Analogue reports / queries as for SQL*Plus
- Use of drill-down and simple graphical reports

What kind of reports are available?

- **Audit Configuration** info about policies, storage and jobs
- **Audit Sessions** reports to analise audit sessions
- **Generate Statements** scripts to generate statements to enable, disable, drop and create policies
- **Top Audit Events** a couple of top audit event reports e.g. by user, policy, action and more

Where to find?

- Available via GitHub Repository oehrlis/oradba SQL Developer XML file unified_audit_reports.xml

4

Special Use Cases

What is special about the use of Unified Audit?

Read Only

What happens if the Database is not opened Read / Write?

Situation where a Database is not opened Read / Write

- Start-up phases such as **nomount** and **mount** or explicitly open in **readonly** mode
- Different Oracle **DataGuard** states

If Audit Data can **not be written** to Database tables it will be written to spillover files

- Location in $ORACLE_BASE/audit/$ORACLE_SID can not be configured
- Transparent access via view *UNIFIED_AUDIT_TRAIL*

Define a strategie to process you Unified Audit spillover files

```
BEGIN
  dbms_audit_mgmt.load_unified_audit_files();
END;
```

Multi Tenancy

Common vs. local Policies - what goes where?

COMMON audit policy

- Policies which are defined on CDB root with CONTAINER=ALL => Valid / Visible in all PDBs
- When enabled the will audit actions for COMMON users in this particular PDB.
- LOCAL user in PDBs will **not be audited** by COMMON audit policies!

LOCAL audit policy

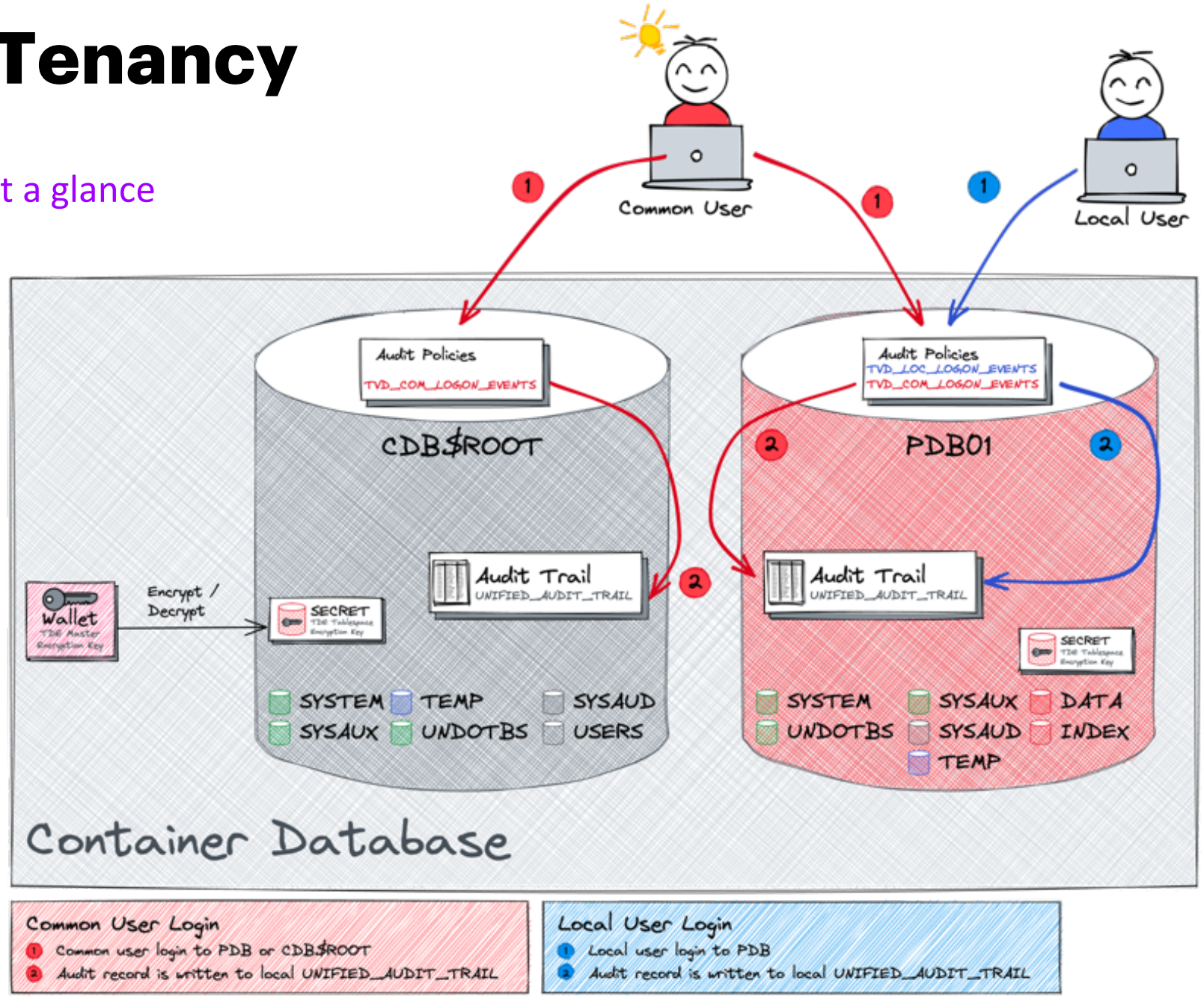
- Defined locally in the PDB or CDB root
- When enabled a local audit policy is valid for LOCAL and COMMON users in this PDB

Define a clear strategie what is done on…

- … common level respectively as common users
- … local / PDB level as local user
- … performed on CDB level e.g. Query Audit Data, Housekeeping etc

Multi Tenancy

Audit Trails at a glance



Proxy Users

A few tricks for proxy users

- Define Audit Policies just for **Proxy Users** by using a condition with SYS Context

```
CREATE AUDIT POLICY oradba_loc_all_act_proxy_usr
ACTIONS ALL
    WHEN '(sys_context(''userenv'',''proxy_user'') IS NOT NULL)'
    EVALUATE PER SESSION ONLY TOPLEVEL;
```

- Get information about **current** and **past proxy user** sessions e.g., join
  - *SESSIONID, PROXY_SESSIONID* from UNIFIED_AUDIT_TRAIL
  - *AUDSID* from V$SESSION

```
SELECT * FROM v$session
WHERE audsid IN ( SELECT sessionid FROM unified_audit_trail WHERE proxy_sessionid <> 0);

SELECT * FROM unified_audit_trail
WHERE sessionid = :SESSIONID OR sessionid = :PROXY_SESSIONID;
```

Database Cloning

Up's why my Audit Trail does not get smaller?

- Audit trails are **never** automatically cleaned up
- Check Audit Records by *DBID*

```
SELECT dbid,count(*) FROM unified_audit_trail u GROUP BY dbid;
```

- Purge foreign Audit Records after cloning using DBMS_AUDIT_MGMT Package
- Consider automatic Post-Clone Action

```
BEGIN
  dbms_audit_mgmt.clean_audit_trail(
    audit_trail_type          =>  dbms_audit_mgmt.audit_trail_unified,
    use_last_arch_timestamp   =>  FALSE,
    database_id               =>  3288252711);
END;
```

- Leaving productive audit data "lying around" can be a **security risk**

Database Export / Import

Should or shouldn't we include Audit Trail in DataPump Exports?

- Unified Audit Trail is part of a full Database export
- Therefore, it can also be imported
- Consider to explicitly **include** or **exclude** it during export or import

```
oracle@cdbua190:/ [CDBUA190] expdp system/manager@pdb1 FULL=YES DIRECTORY=dpdump DUMPFILE=pdb1_full.dmp
LOGFILE=pdb1_full.log REUSE_DUMPFILES=yes

Export: Release 19.0.0.0.0 - Production on Tue Sep 5 04:53:13 2023
Version 19.19.0.0.0

Copyright (c) 1982, 2023, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Starting "SYSTEM"."SYS_EXPORT_FULL_01":  system/********@pdb1 FULL=YES DIRECTORY=dpdump DUMPFILE=pdb1_full.dmp
LOGFILE=pdb1_full.log REUSE_DUMPFILES=yes
Processing object type DATABASE_EXPORT/EARLY_OPTIONS/VIEWS_AS_TABLES/TABLE_DATA
...
Processing object type DATABASE_EXPORT/AUDIT_UNIFIED/AUDIT_POLICY
Processing object type DATABASE_EXPORT/AUDIT_UNIFIED/AUDIT_POLICY_ENABLE
Processing object type DATABASE_EXPORT/POST_SYSTEM_IMPCALLOUT/MARKER
. . exported "SYS"."KU$_USER_MAPPING_VIEW"                6.132 KB      41 rows
. . exported "AUDSYS"."AUD$UNIFIED":"SYS_P241"            27.81 MB   13262 rows
```

Top Level Statements

Top Level does not necessarily mean just the one statement

Intended for PL/SQL Procedure **only**

- Sub queries are not creating Audit Statements
- Reduce the number of Audit Events

Does **not work** for VIEWS or regular queries

- If Audit Action is set for SELECT any select will create an Audit Record
- Browsing the Database using OEM, SQL Developer etc can be quite chatty
- Find a trade of between full statement Audit and

Mandatory Policy

Search for hints and traces in Oracle 23c Free

New hidden parameters available:

- **_enable_protected_audit_policy** Allow Protected Unified Audit Policy Enforcement

New column in AUDIT_UNIFIED_POLICIES see desc

- PROTECTED not yet documented in Oracle® Database Database Reference 23c

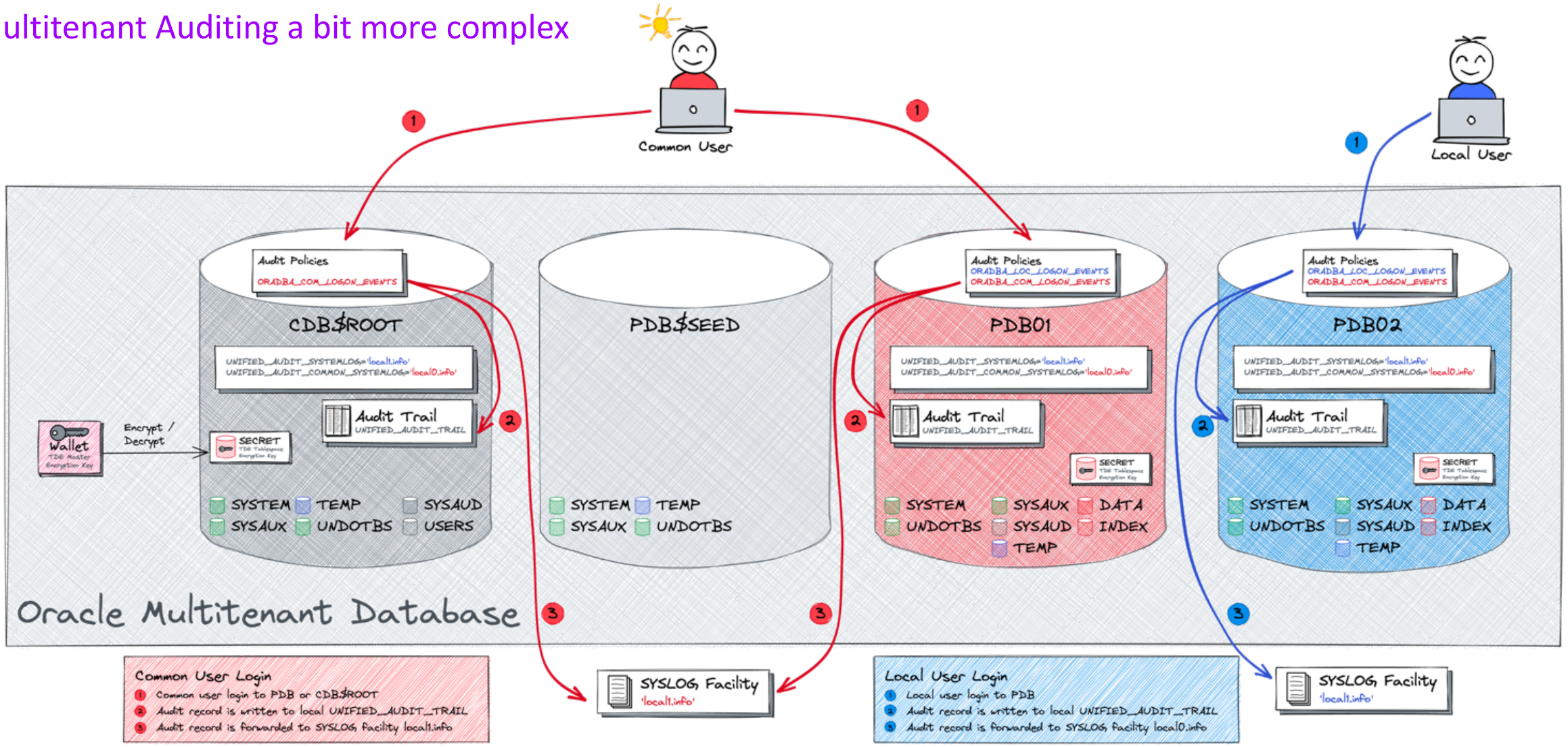
Presumably to enforce Audit Policies in PDBs

- Policy defined by SYSDBA / Common User
- Not changeable within PDB by Audit Admin

```
SQL> DESC audit_unified_policies
 Name                      Type
 ------------------------- -------------
 POLICY_NAME               VARCHAR2(128)
 AUDIT_CONDITION           VARCHAR2(4000)
 CONDITION_EVAL_OPT        VARCHAR2(9)
 AUDIT_OPTION              VARCHAR2(128)
 AUDIT_OPTION_TYPE         VARCHAR2(18)
 OBJECT_SCHEMA             VARCHAR2(128)
 OBJECT_NAME               VARCHAR2(128)
 OBJECT_TYPE               VARCHAR2(23)
 COMMON                    VARCHAR2(3)
 INHERITED                 VARCHAR2(3)
 AUDIT_ONLY_TOPLEVEL       VARCHAR2(3)
 ORACLE_SUPPLIED           VARCHAR2(3)
 PROTECTED                 VARCHAR2(3)
 COLUMN_NAME               VARCHAR2(128)
```

Syslog Integration

Multitenant Auditing a bit more complex



Syslog Integration

Don't expect too much...

- SYSLOG is limited by design i.e., not only Oracle
  - In terms of record length / content
  - In terms of possible SYSLOG facilities to be configured
- Define a clearly defined Use Case to forward audit information to SYSLOG
  - E.g., SOCs integration, Alerting etc
- Configuration is simple and straight forward
- Full Audit Event information is **always** in UNIFIED_AUDIT_TRAIL

```
host sudo grep -i 2578688223 /var/log/oracle_common_audit_records.log
Mar 23 14:49:44 localhost journal: Oracle Unified Audit[17838]: LENGTH: '204' TYPE:"4"
DBID:"1612911514" SESID:"2578688223" CLIENTID:"" ENTRYID:"1" STMTID:"1" DBUSER:"SYSTEM"
CURUSER:"SYSTEM" ACTION:"100" RETCODE:"0" SCHEMA:"" OBJNAME:""
PDB_GUID:"86B637B62FDF7A65E053F706E80A27CA"
```

Issues?

Now and then there are issues…

- Open a Service request with a **clearly** defined test case
  - No excuse to not open an SR
- My past 2 issues have been solved within weeks with One-Off Patches
  - All patches have been part of the next RU

A few Examples

- Bug 30769454 - Policy Created For Some Actions Are Not Showing In Audit_Unified_Policies (Doc ID 30769454.8)
- Bug 35562961 - DB 19.19: ORA-28267: Invalid Namespace Value - audit_unified_contexts (Doc ID 35562961.8)
- Unified Audit is not “really” read only, just marked internally as read only table

6

Migration

Any special tasks when migrating databases?

From Legacy to Unified

Unified Audit mix Mode the data multiplier

- Default Mode when creating a database
  - Traditional **and** Unified Audit settings are active
- Check status by query V$OPTION

```
SQL> SELECT value FROM v$option WHERE PARAMETER = 'Unified Auditing';
VALUE
----------------------------------------------------------------
TRUE
```

- Pure Mode enabled by linking Oracle binaries see 1567006.1
  - Mix Mode only for a short transition
- Scripts available to Convert raditional **into** Unified Audit settings
  - 2909718.1 Traditional to Unified Audit Syntax Converter - Generate Unified Audit Policies from Current Traditional Audit Configuration

Database Migration

Not everything that is new is also good

Oracle Unified Audit needed 1-2 major releases to grow

- Initial Release in 12.1 did use an approach with buffer / queue
- Bad performance

Restructure of Unified Audit Trail to an internal relational table

- Mandatory Migration of Audit Trail when going from 12.1 to newer version
- 2212196.1 How To Transfer Unified Audit Records To An Internal Relational Table

7

Central Audit Management

What to do with all the data?

Custom Solutions

What ever you like to build…

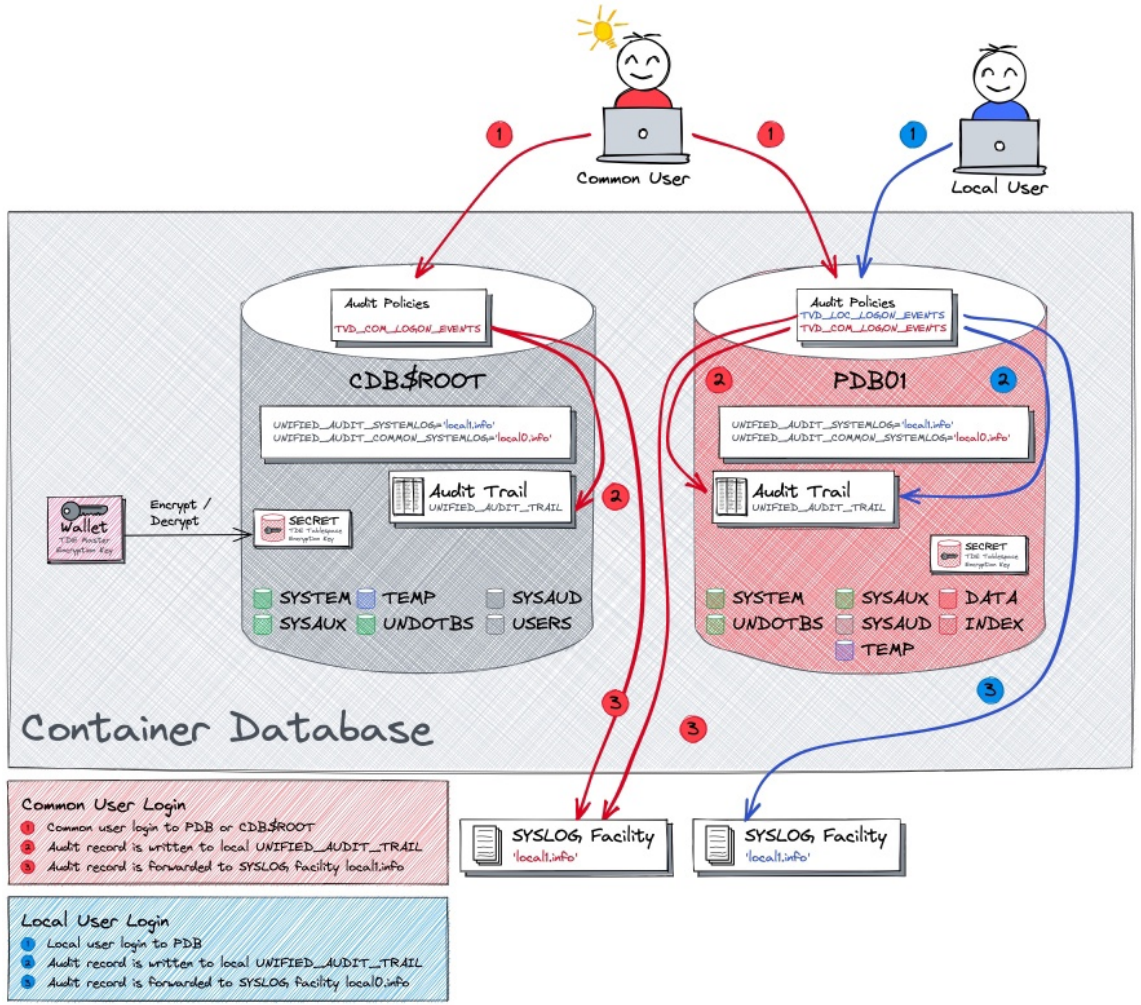
The solutions are usually **limited** to…

- Central Repository
- Reporting
- SOC (Security Operation Center) Integration

Possible Solution Approaches

- **Splunk** Audit data Collection
- **Elasticsearch** or ELK Stack
- **SYSLOG** integration

Usually **no** Audit Policy Management and Database Security Assessment



Custom Solutions

What ever you like to build…

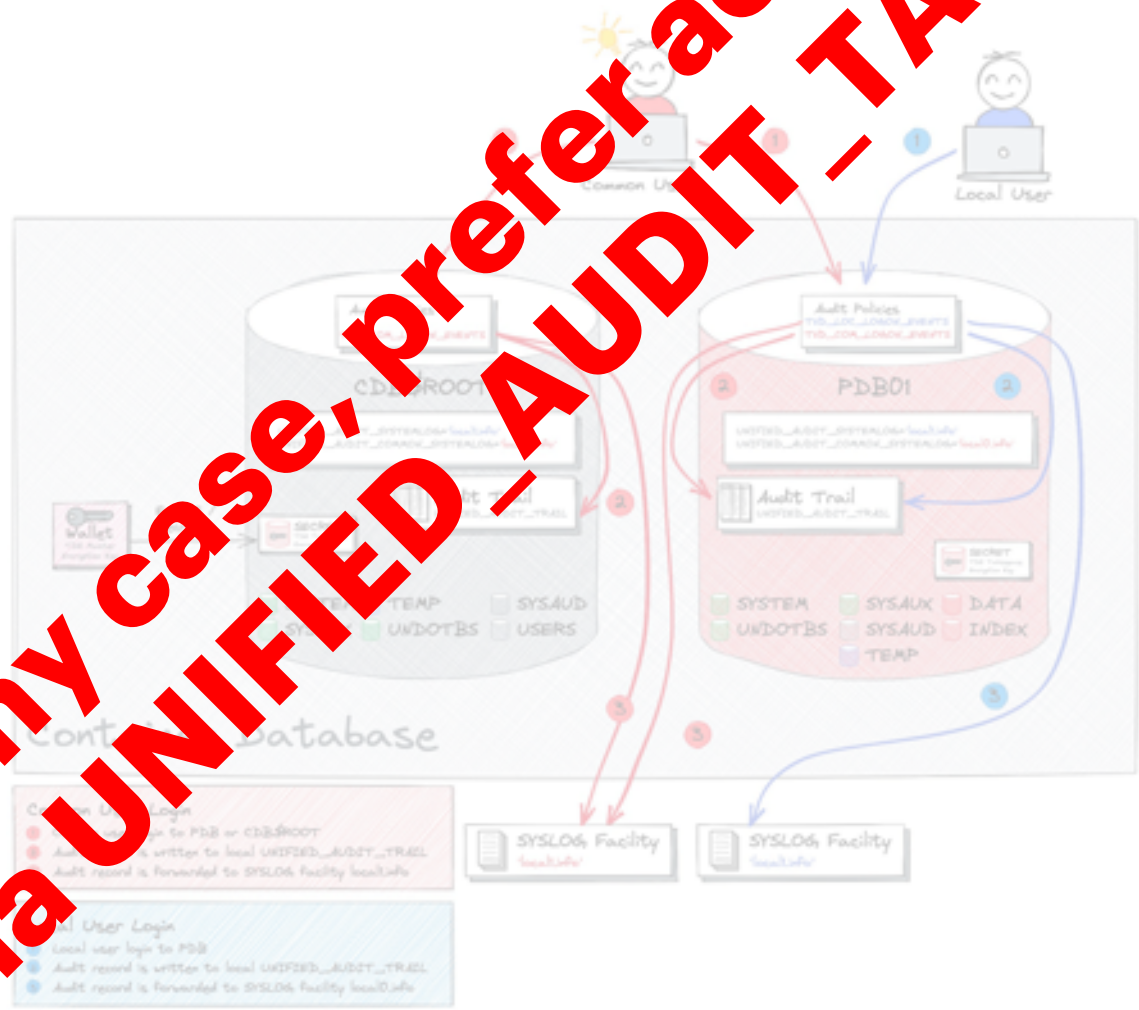
The solutions are usually **limited** to…

- Central Repository
- Reporting
- SOC (Security Operation Center) Integration

Possible Solution Approaches

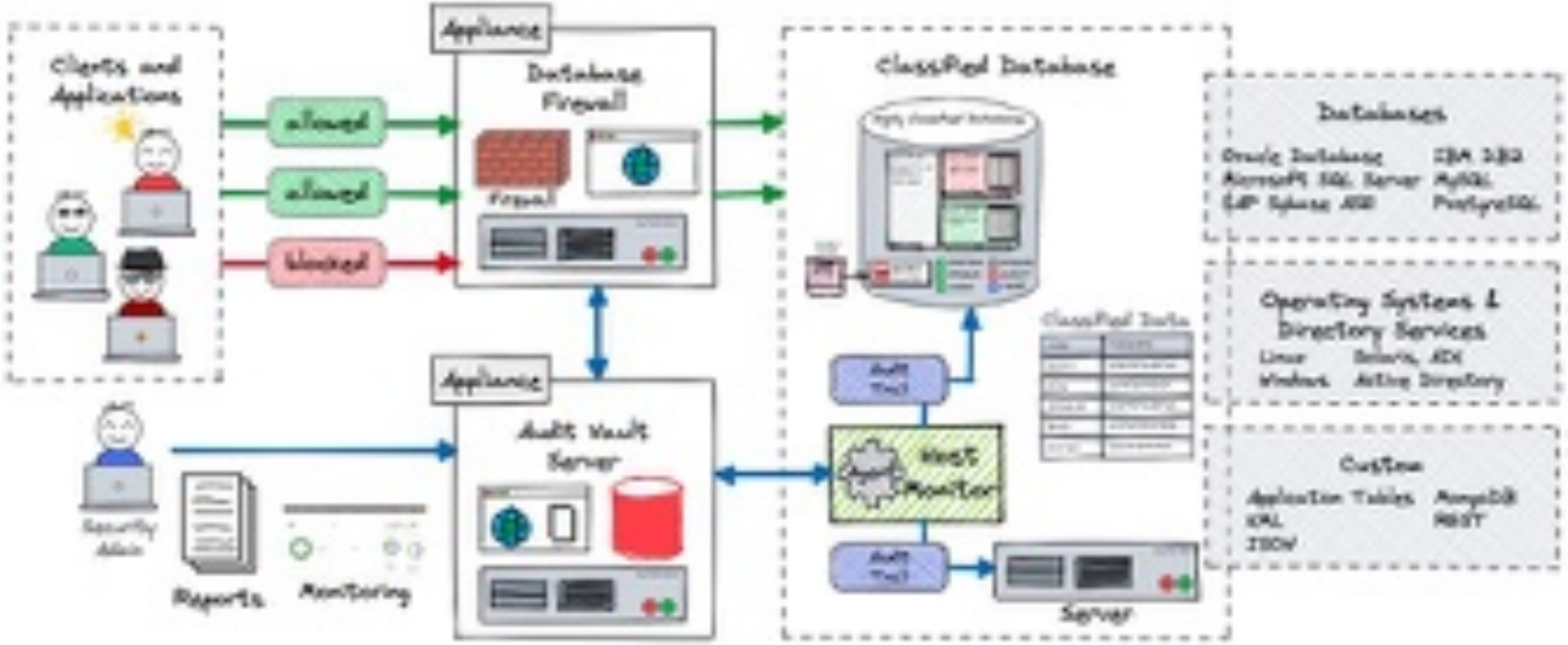
- **Splunk** Audit data Collection
- **Elasticsearch** or ELK Stack
- **SYSLOG** integration

Usually **no** Audit Policy Management and Database Security Assessment



Oracle AVDF Architecture

Components at a glance



Oracle Data Safe

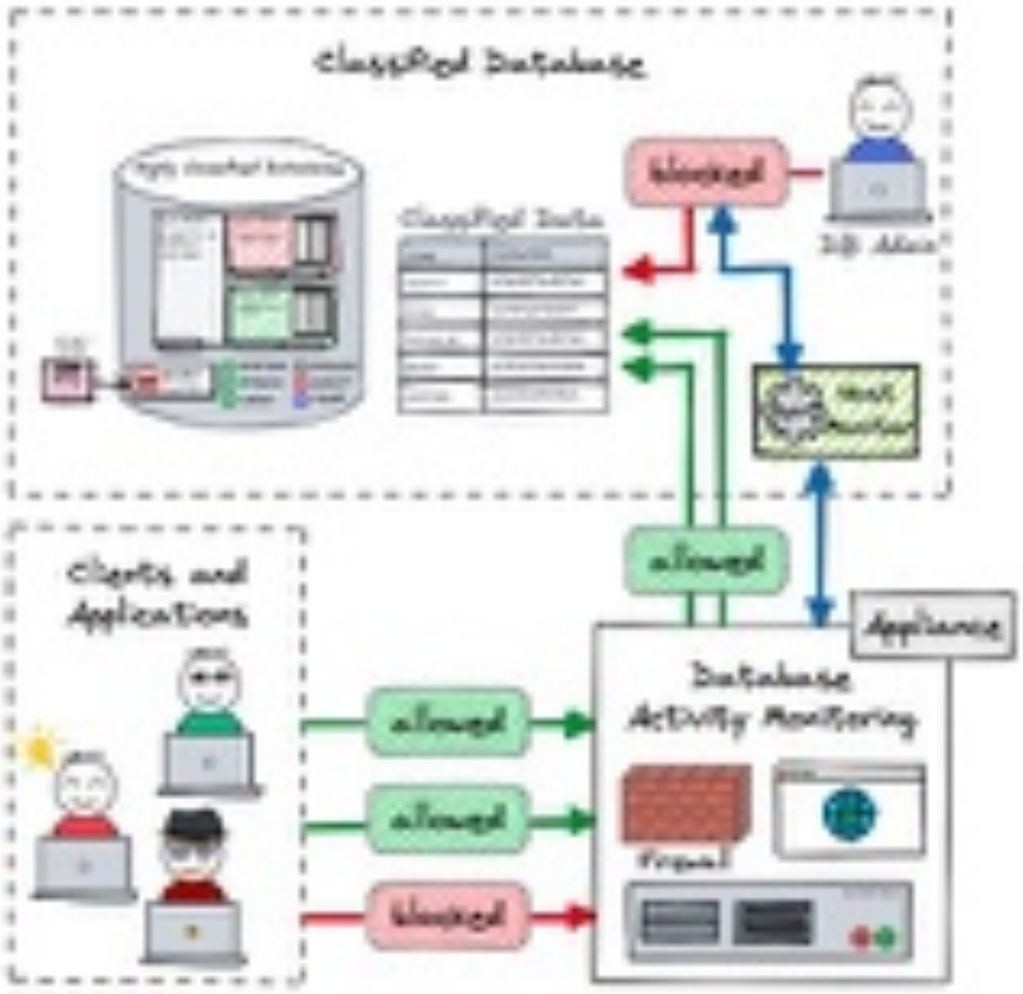
Cloud based Database Security Service

- **Security Assessment** to assess the security of database configurations
- **User Assessment** to assess the security of database users and identify high risk users
- **Data Discovery** to identify sensitive data in databases
- **Data Masking** provides a way to mask sensitive data so that the data is safe for non-production purposes
- **Activity Auditing** lets audit user activity on databases so one can monitor database usage
- **Alerts** keep one informed
- Available for cloud and on-premises databases

Source: https://blogs.oracle.com

Database Activity Monitoring

Control what happens within the databases



- **Similar** functionality to the database firewall
- inspect SQL **Traffic** to Database
- Monitor local activity with **Host Monitor**
- Multi Database Support
- Limitation in SQL Net Traffic encryption
- No Oracle Audit integration

Third party products like

- Imperva **SecureSphere** Data Security
- IBM Security **Guardium**
- Sentrigo Hedgehog aka McAfee DAM aka ...

Conclusion

Have you found some ideas for your own Unified Audit ambitions?

Oracle Unified Audit is a **good thing**

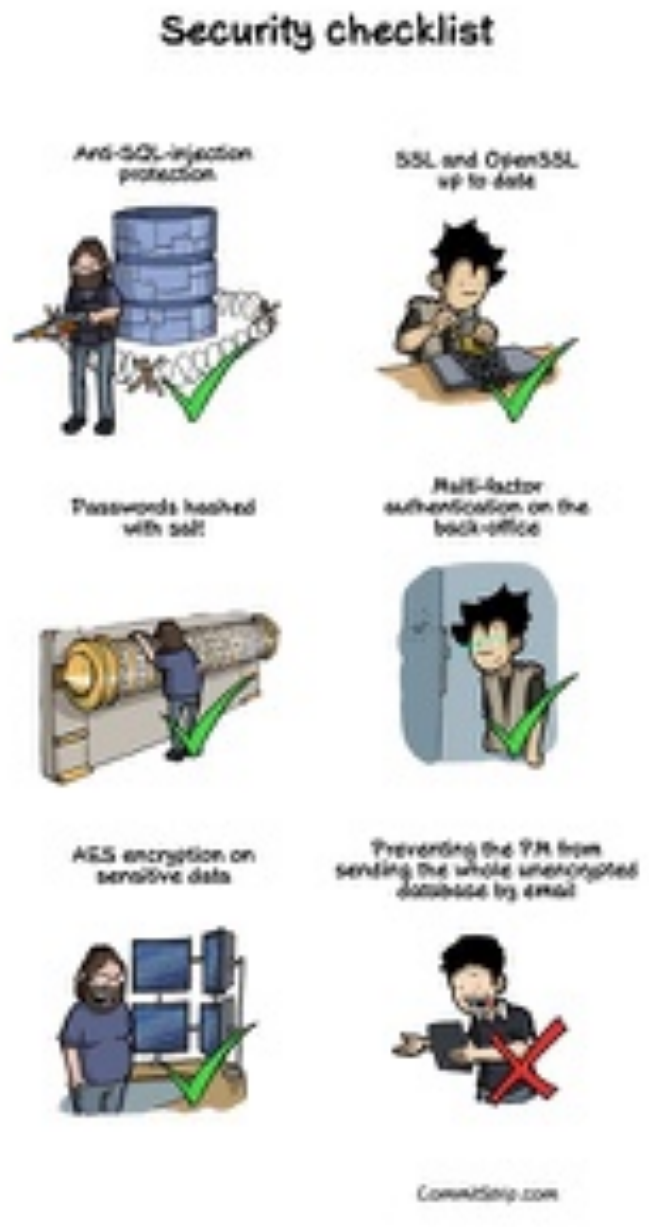
- The Audit Policy greatly simplifies the deployment of security Requirement
- Only one place where the Audit Data is filed
- Much lower impact on performance compared to traditional Audit

The latest version of Oracle Unified Audit is **fundamentally robust**

- Nevertheless, problems occur from time to time. i.e., bugs, but also configuration errors

A few Features are **Still Missing**

- Online update of Audit Policies, i.e., also for current sessions => 21c / 23c
- Mandatory Audit Policies in Container Databases



A solid User and Role Concept is a mandatory prerequisite for successful database auditing.

Thank You

Oracle Unified Audit

Documentation, White Papers, Support Notes and other Links

- *Oracle® Database Security Guide 21c* Monitoring Database Activity with Auditing
- Oracle White Paper Oracle Database Unified Audit - Best Practice Guidelines
- 2351084.1 Primary Note For Database Unified Auditing
- 1299033.1 Primary Note For Oracle Database Auditing
- 2909718.1 Traditional to Unified Audit Syntax Converter
- 1567006.1 How To Enable The New Unified Auditing In 12c?
- 2750986.1 19c: How to export unfied audit trail using datapump
- 1582627.1 How To Purge The UNIFIED AUDIT TRAIL
- 2212196.1 How To Transfer Unified Audit Records To An Internal Relational Table
- **OraDBA** Blog Post Category for Oracle Unified Audit
- **GitHub** Repository oehrlis/oradba SQL Developer

>