Easy Audit Data Analysis

SQL Developer Reports

Stefan Oehrli

Stefan Oehrli – Data Platforms

Oracle ACE Pro

stefan.oehrli@accenture.com

Terraform ASSOCIATE – HashiCorp CERTIFIED

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. SQL*Plus Reporting
3. SQL Developer Reporting
4. Good Practice
5. Conclusion

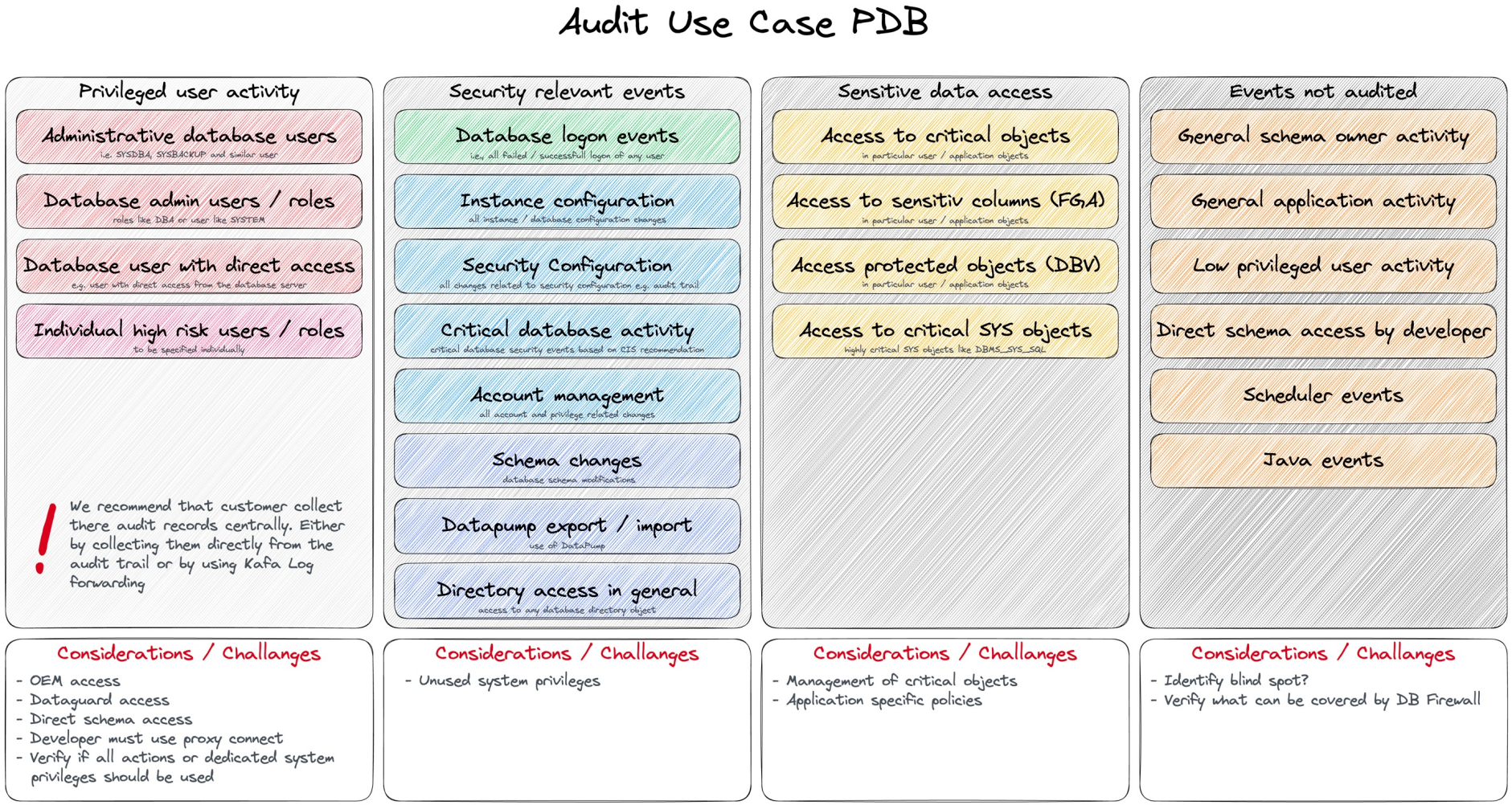
1

Introduction

What about the Security Features in 23c?

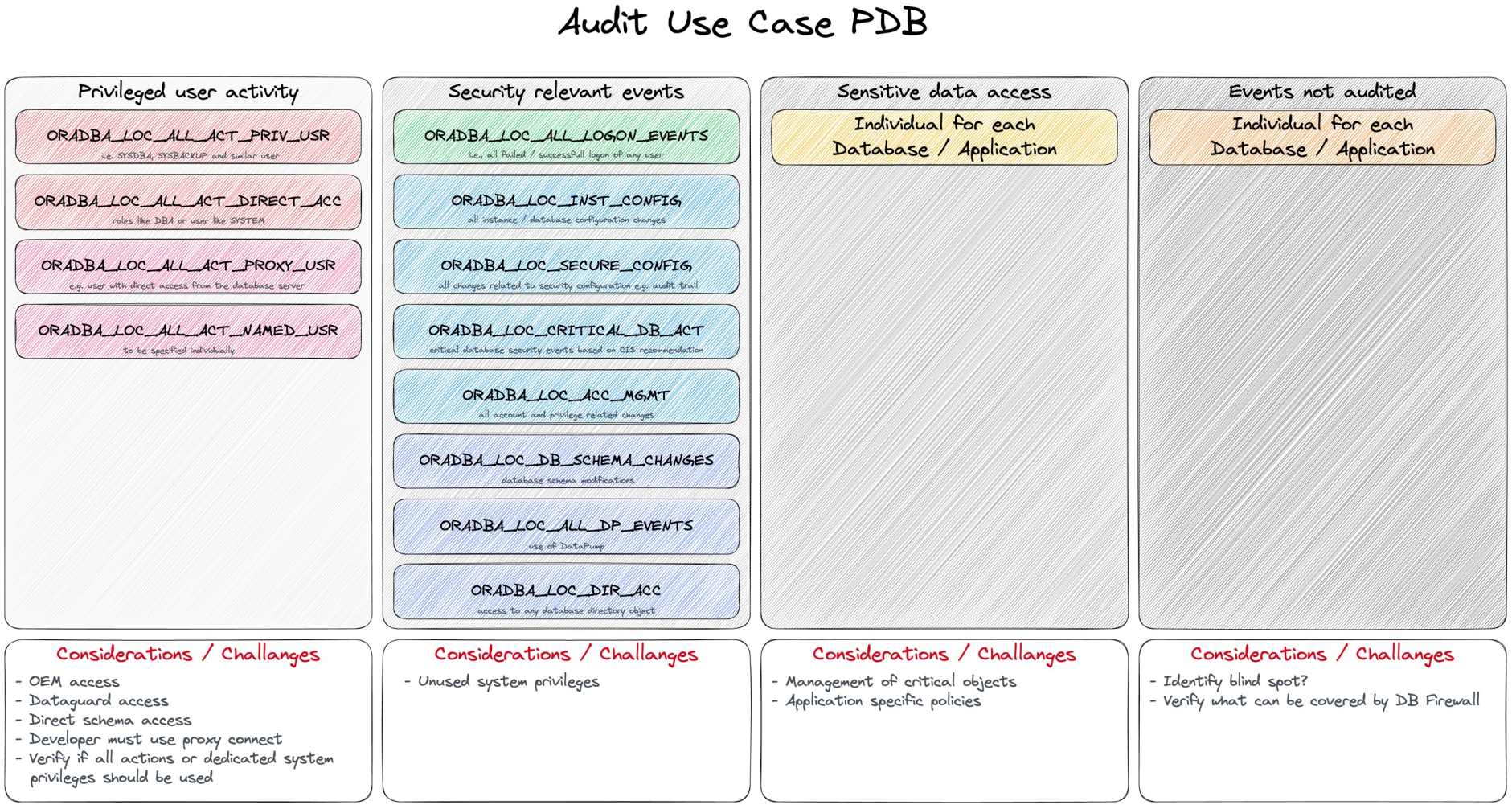
Audit Use Cases

What kind of Audit Events should be covered?



Audit Use Cases

Which policies should be enabled?



Problem

Too much, too little, neither ideal

- Currently **too much** audit data is generated
  - All administration and monitoring tasks run as **SYSDBA**
- Waste of **space and resources** in the database
  - Do we need so much audit data for so long?
- **High costs** in post processing due to the transactions / data volume
  - Amount could be reduced by filter data when loaded from database
- Analysis of the audit data is like *“looking for a needle in a haystack”*

2

SQL*Plus Reporting

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*Plus Reporting 1/4

SQL*Plus Script to dive into audit data

Script	Purpose
caua_pol.sql	Create custom local audit policies policies
cdua_init.sql	Initialize Audit environment (create tablespace, reorganize tables, create jobs)
daua_pol.sql	Disable all audit policies and drop all non-Oracle maintained policies
iaua_pol.sql	Enable custom local audit policies policies
saua_as.sql	Show audit sessions for audit any type
saua_asbck.sql	Show audit sessions for audit type RMAN
saua_asdbv.sql	Show audit sessions for audit type Database Vault
saua_asdet.sql	Show entries of a particular audit session with unified_audit_policies
saua_asdetsql.sql	Show entries of a particular audit session with SQL_TEXT
saua_asdp.sql	Show audit sessions for audit type Datapump
saua_asfga.sql	Show audit sessions for audit type Fine Grained Audit

SQL*Plus Reporting 2/4

SQL*Plus Script to dive into audit data

Script	Purpose
saua_asstd.sql	Show audit sessions for audit type Standard
saua_critobj.sql	Show recently accessed critical objects
saua_critprivs.sql	Show recently used critical privileges
saua_grants.sql	Show recently granted privileges
saua_info.sql	Show information about the audit trails
saua_logfail.sql	Show failed logins
saua_pol.sql	Show local audit policies policies. A join of the views AUDIT_UNIFIED_POLICIES and AUDIT_UNIFIED_ENABLED_POLICIES
saua_report.sql	Create a simple report by running all show saua_xxxx.sql show scripts
saua_tabsize.sql	Show Unified Audit trail table and partition size
saua_teact.sql	Show top unified audit events by action for current DBID

SQL*Plus Reporting 3/4

SQL*Plus Script to dive into audit data

Script	Purpose
saua_tecli.sql	Show top unified audit events by client_program_name for current DBID
saua_tedbid.sql	Show top unified audit events by DBID
saua_tehost.sql	Show top unified audit events by userhost for current DBID
saua_teobj.sql	Show top unified audit events by object_name for current DBID
saua_teobjusr.sql	Show top unified audit events by Object Name without Oracle maintained schemas for current DBID
saua_teosusr.sql	Show top unified audit events by os_username for current DBID
saua_teown.sql	Show top unified audit events by object_schema for current DBID
saua_tepol.sql	Show top unified audit events by unified_audit_policies for current DBID
saua_tepoldet.sql	Show top unified audit events by unified_audit_policies, dbusername, action for current DBID
saua_teusr.sql	Show top unified audit events by dbusername for current DBID

SQL*Plus Reporting 4/4

SQL*Plus Script to dive into audit data

Script	Purpose
saua_user.sql	Show recently created users
sdua_crpolstm.sql	Generate statements to create all audit policies as currently set in AUDIT_UNIFIED_ENABLED_POLICIES
sdua_dipolstm.sql	Generate statements to disable all audit policies as currently set in AUDIT_UNIFIED_ENABLED_POLICIES
sdua_drpolstm.sql	Generate statements to drop all audit policies as currently set in AUDIT_UNIFIED_ENABLED_POLICIES
sdua_enpolstm.sql	Generate statements to enable all audit policies as currently set in AUDIT_UNIFIED_ENABLED_POLICIES
sdua_prgstm.sql	Generate Unified Audit trail storage purge statements
sdua_stostm.sql	Generate Unified Audit trail storage usage modification statements
sdua_usage.sql	Show Unified Audit trail storage usage

3

SQL Developer Reporting

Simple and straight forward analysis of the audit data

SQL Developer Reporting

Let's dive into the slightly more pleasant Audit Reporting

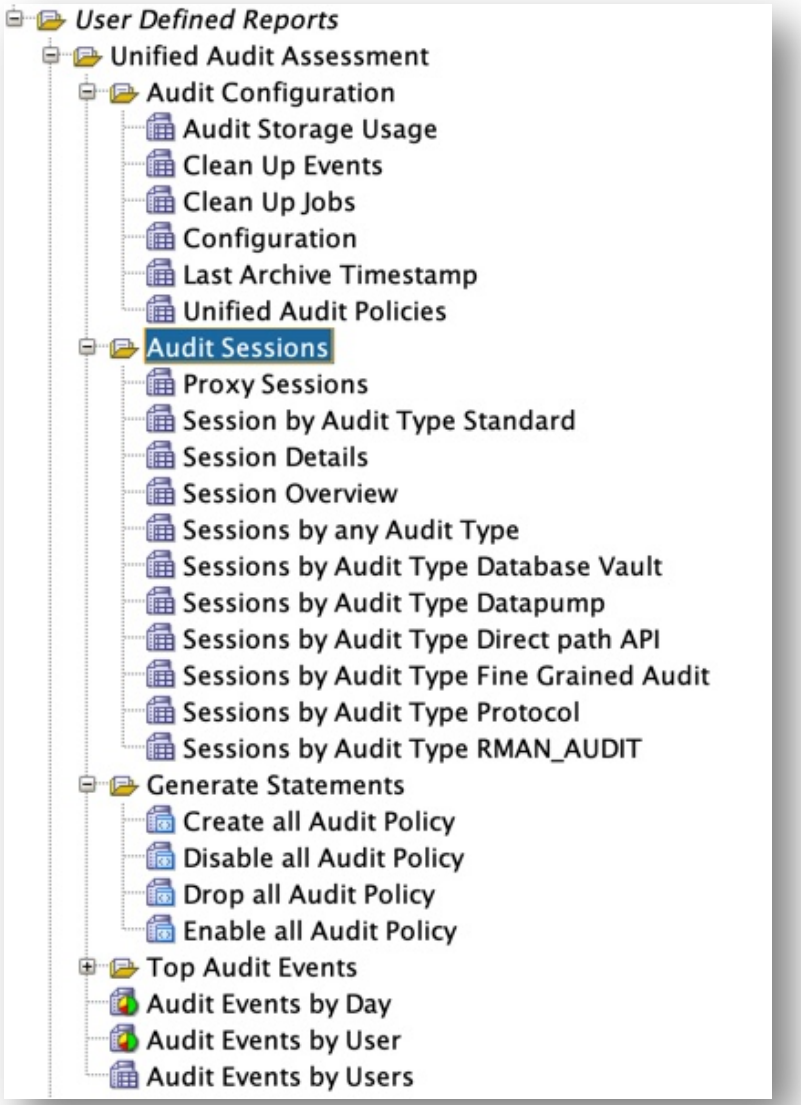
- Analogue reports / queries as for SQL*Plus
- Use of drill-down and simple graphical reports

What kind of reports are available?

- **Audit Configuration** info about policies, storage and jobs
- **Audit Sessions** reports to analyze 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

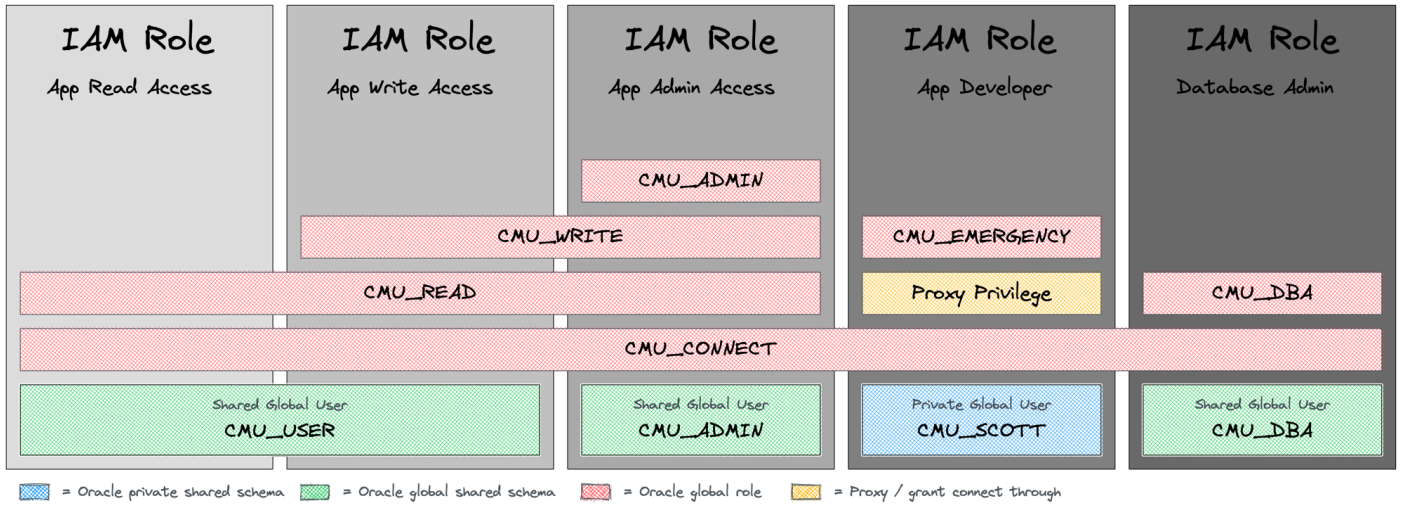
Good Practice

What has worked well for Unified Audit?

User and Role Concept

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

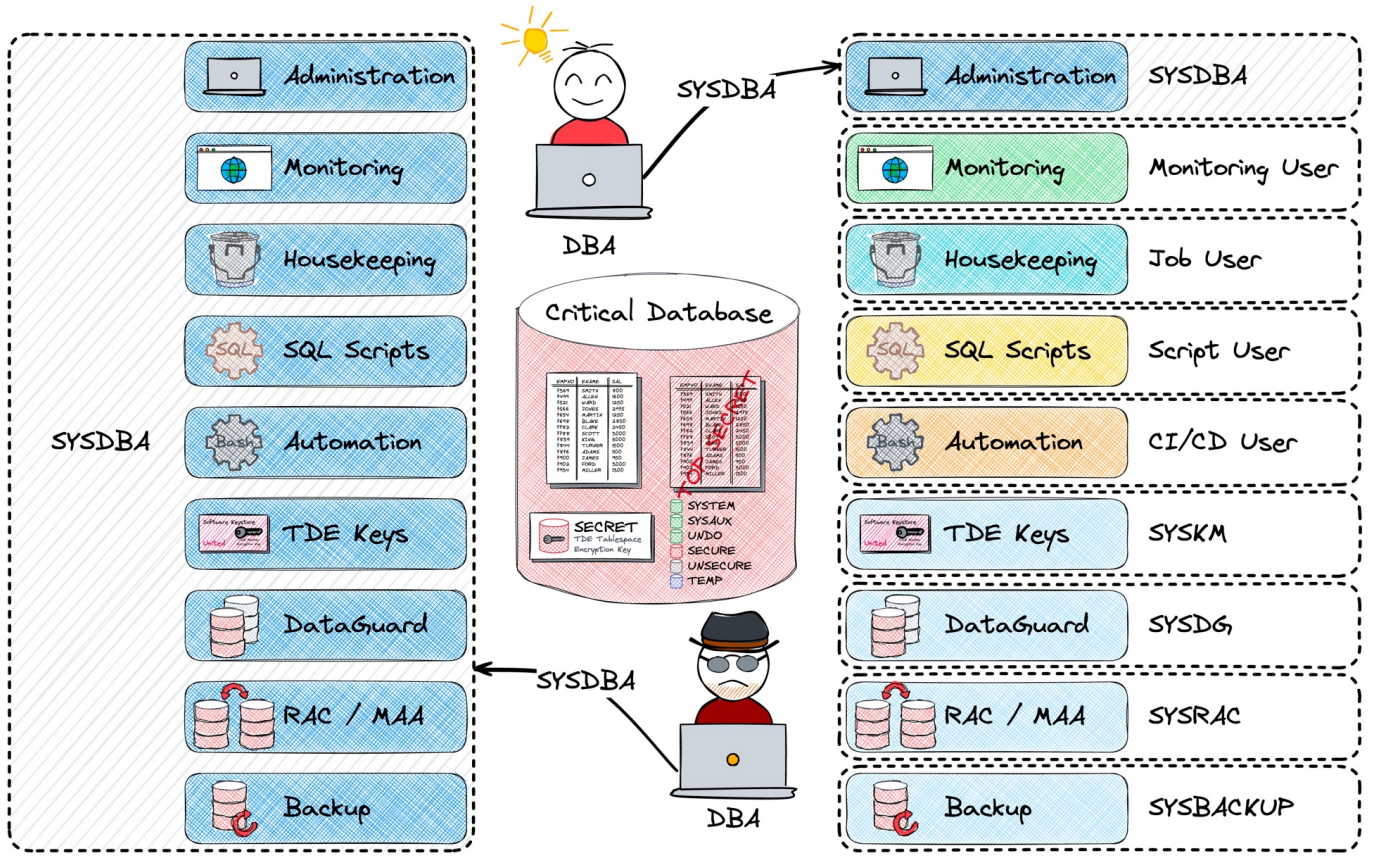
- Definition of **distinguished** user Groups and Roles
- Implementation of the Principle of **Least Privilege**
  - Use tools like privilege capture to analyse
- Do not use SYSDBA / DBA for “everything”
  - Appropriate use of SYSDG, SYSKM, etc.



SYSDBA for All...

Segregation of Duties also without Database Vault

- Do **not run** everything as SYSDBA
  - Impossible to distinguish the activities
- Implement **least privileges principle**
  - Grant just as many privileges as necessary
- Use **dedicated admin privileges** e.g. SYSDG, SYSBACKUP, SYSRAC etc.
- Create dedicated operation accounts
  - Monitoring user
  - Job / Batch user
- Use **privilege capture** for the needs analysis



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

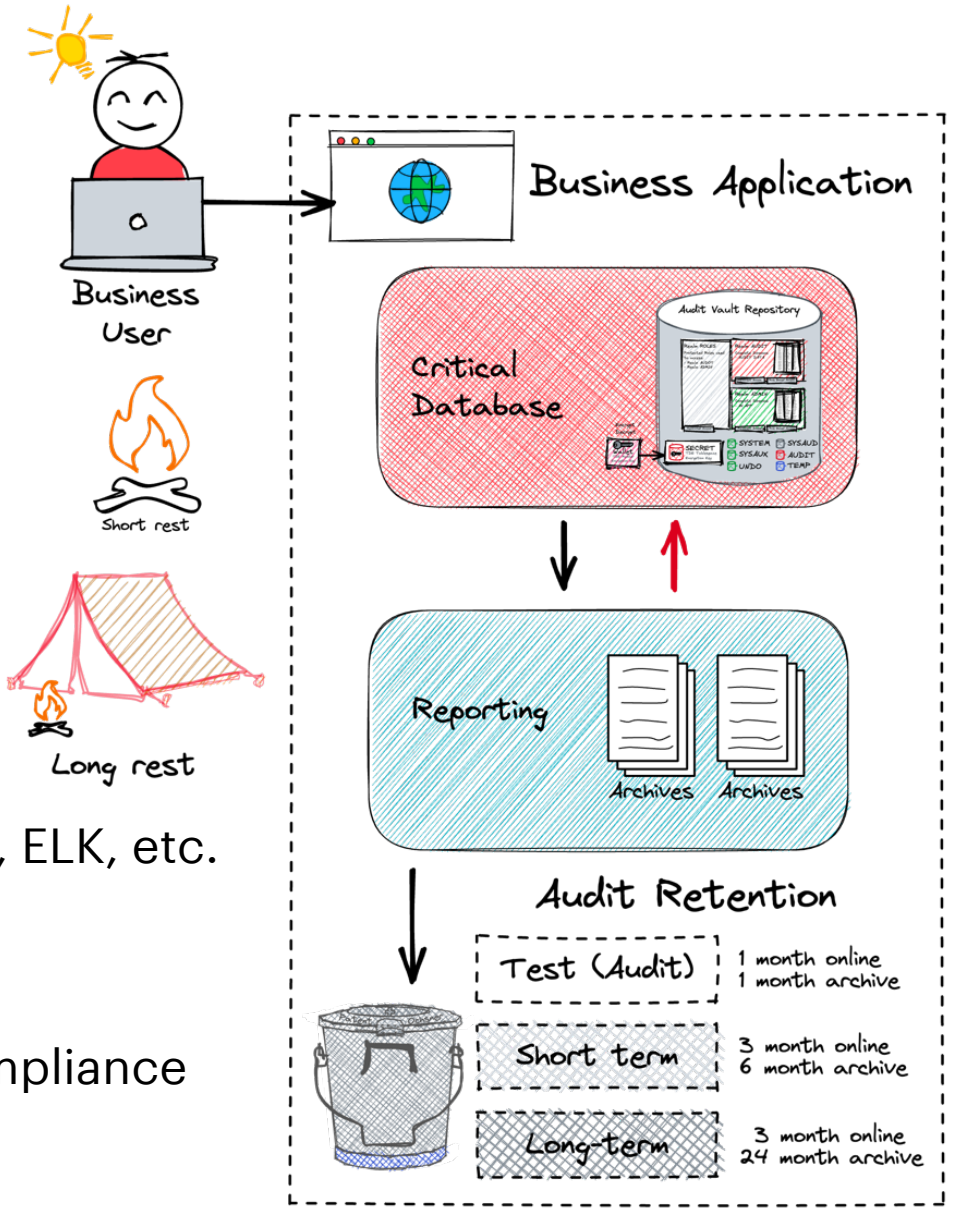
Central storage of raw Audit Data

- 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

Conclusion

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

Oracle Unified Audit is a **good thing**

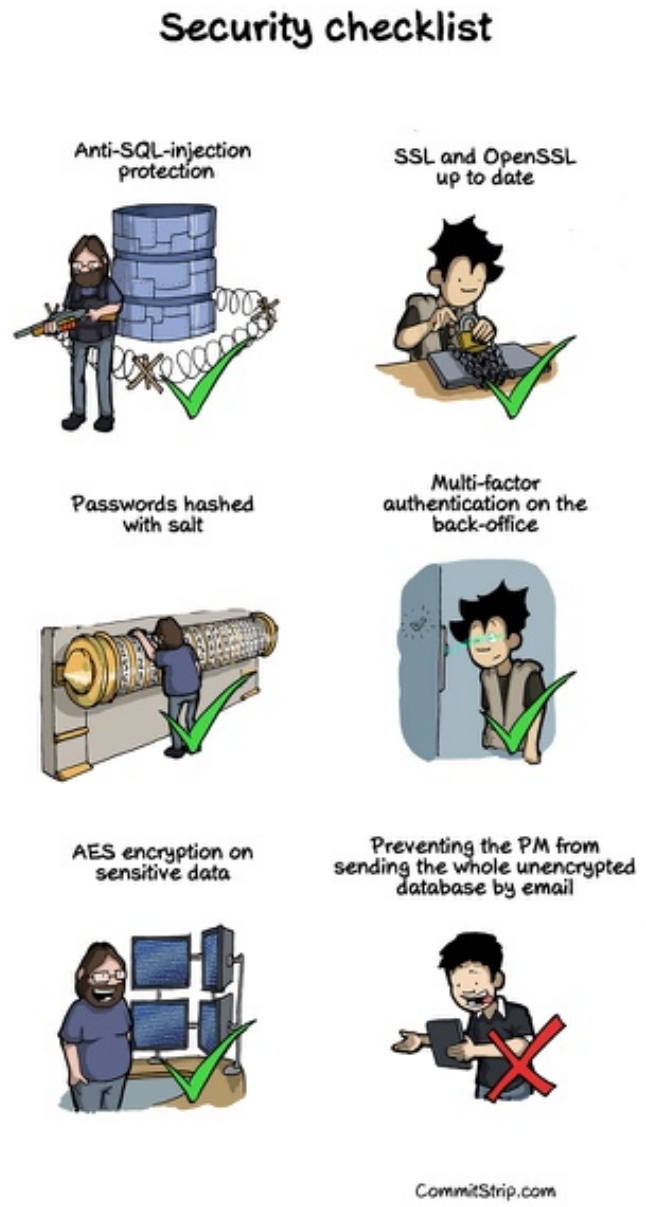
- The Audit Policy greatly simplifies the deployment of security Requirement
- Only one place where the Audit Data is filed
- Much lower impact on performance compared to traditional Audit

A good and **fundamentally robust** concept is mandatory

- What has to be audited?
- Least privilege principle

The simple set of script can help to **drill down audit events**

- SQL*Scripts to work on command line
- SQL Developer Reports to interactively analyze audit data.



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

Oracle Unified Audit

Documentation, White Papers, Support Notes and other Links

- *Oracle® Database Security Guide 23c* 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

Thank You