

# Oracle AVDF

Oracle Audit Vault and Database Firewall  
at a glance

**Dienstag, 4. April 2023**

Stefan Oehrli

# Stefan Oehrli – Data Platforms

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)



# 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 AVDF

What to expect with the latest version of Oracle AVDF?

- 1** Introduction
- 2** AVDF in a Nutshell
- 3** Use Cases
- 4** Latest Enhancements
- 5** Best Practice
- 6** Licensing
- 7** Other Solutions
- 8** Conclusion



# 1

## Introduction

Why is Oracle AVDF needed at all?

# Introduction

## Motivation for Oracle ADVF

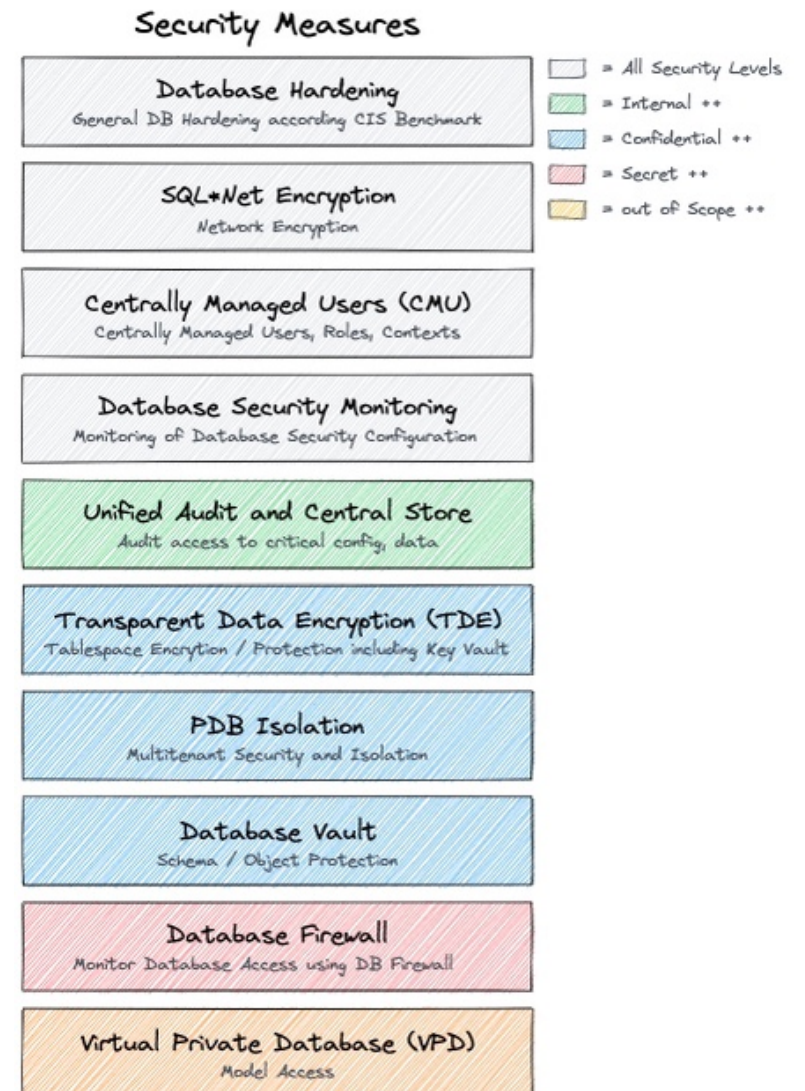
Why Database Security at all?

- 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



# 2

## **AVDF in a Nutshell**

Architecture, Structure  
and Functionality of  
AVDF

# Software Appliance

Everything bundled...

**Oracle** provides software as Appliance

- ISO image containing OS, Database and Application
- Dedicated ISO for Audit Vault and Database Firewall

**Customer** delivers the hardware

- Dedicated x86-64 server or virtual machine
- Simplified setup to install everything in one step
- Reduced Access / Segregation of Duties

**Oracle Cloud** deployment

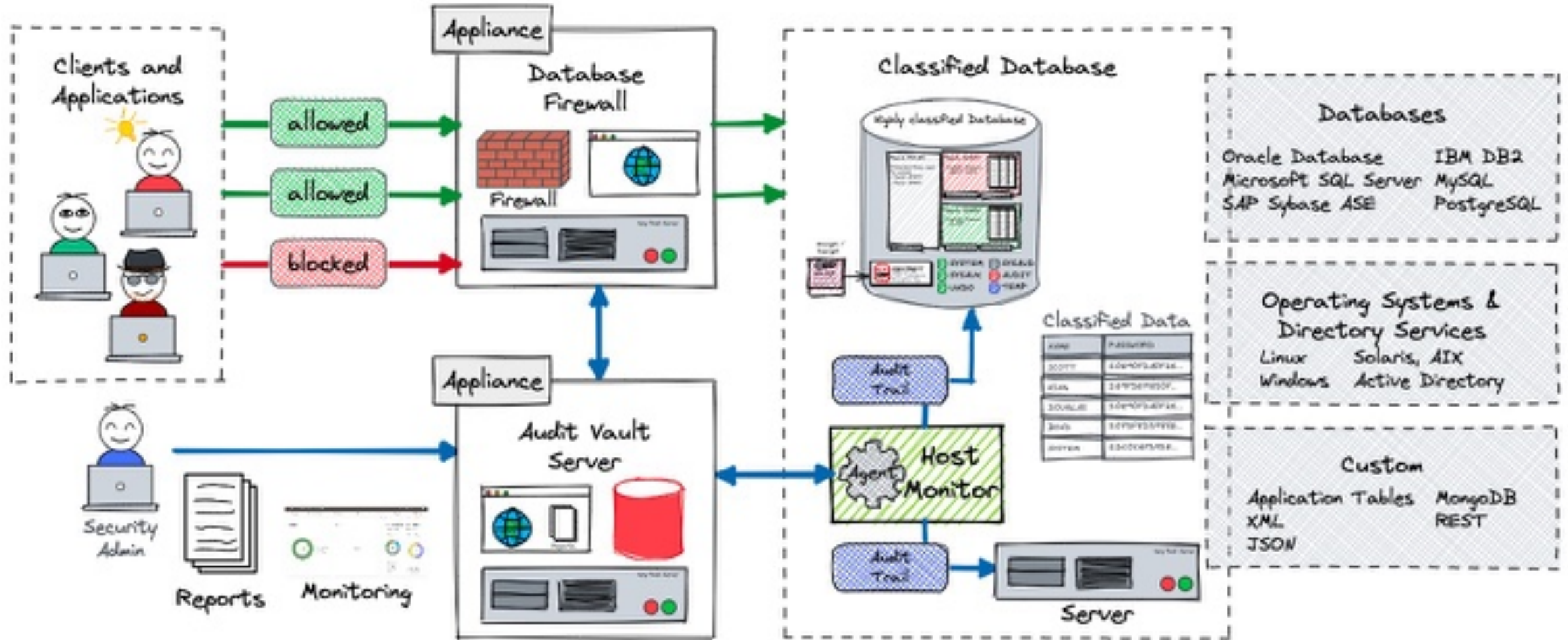
- Simplified installation based on Market place images
- Ideal for tests and proof of concepts





# Oracle AVDF Architecture

## Components at a glance



# Oracle AVDF Architecture

## Out-of-the-Box Plug-ins and Features Supported

Target Version	Audit Trail Collection	Audit Policy Creation	Stored Procedure Auditing	Audit Trail Clean up	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic
Oracle Database 11.2	✓	✓	✓	✓	✓	✓	✓
Oracle Database 12c, 18c, 19c	✓	✓	✓	✓	✓	✓	✓
MS SQL Server 2012, 2014, 2016, 2017, 2019	✓		✓	✓	✓	✓	✓
MS SQL Server 2012 R2 (Windows Clustered)	✓		✓	✓			
SAP Sybase ASE 15.7, 16	✓		✓		✓	✓	
IBM 10.5, 11.1, 11.5	✓			✓	✓	✓	✓
MySQL 5.6, 5.7, 8.0	✓			✓	✓	✓	
PostgreSQL 9.6 to 11.8, 12, 13	✓			✓	✓	✓	



# Oracle AVDF Architecture

## Out-of-the-Box Plug-ins and Features Supported

Target Version	Audit Trail Collection	Audit Policy Creation	Stored Procedure Auditing	Audit Trail Clean up	Database Firewall	Host Monitor Agent	Native Network Encrypted Traffic
Oracle Solaris 11.x up to 11.4 on	✓					✓	
Oracle Linux 6.0 - 6.10, 7.0 - 7.3, 7.4, 7.5, 7.8, 8, 8.2, 8.3, 9	✓					✓	
RedHat Linux 6.8 - 6.10, 7.3 - 7.8, 9	✓					✓	
IBM AIX 7.1 TL5, 7.2 (TL2, TL3, TL4) on Power Systems	✓					✓	
Microsoft Windows Server 2012, 2012 R2, 2016, and 2019	✓						
Microsoft Active Directory 2012, 2012 R2, and 2016	✓						
Oracle ACFS 12c	✓						



# Segregation of Duty

Enforcement of the separation of responsibilities

## AV Administrator

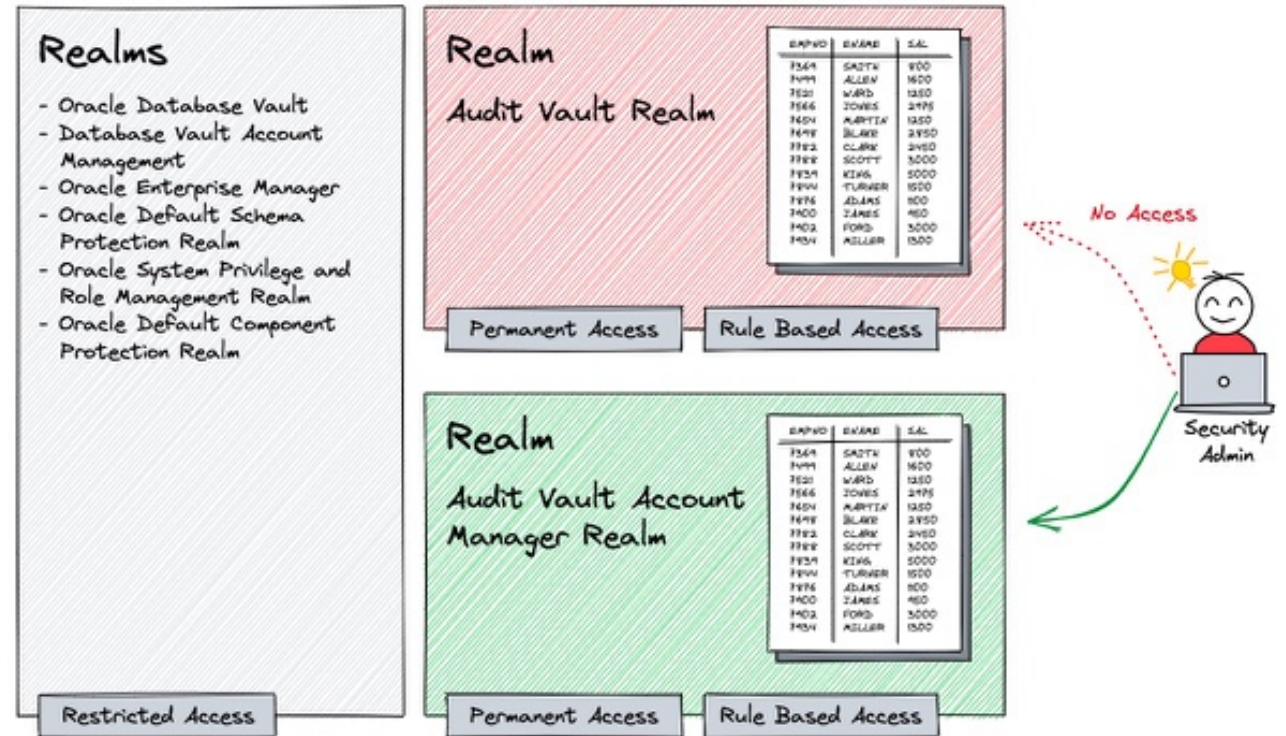
- Maintain AVDF infrastructure
- Deploy AV agents

## AV Auditor

- Define audit policies
- Define firewall rules
- Report and Assessments

## Infrastructure Admin

- Operate and maintain Infrastructure e.g., storage, vm



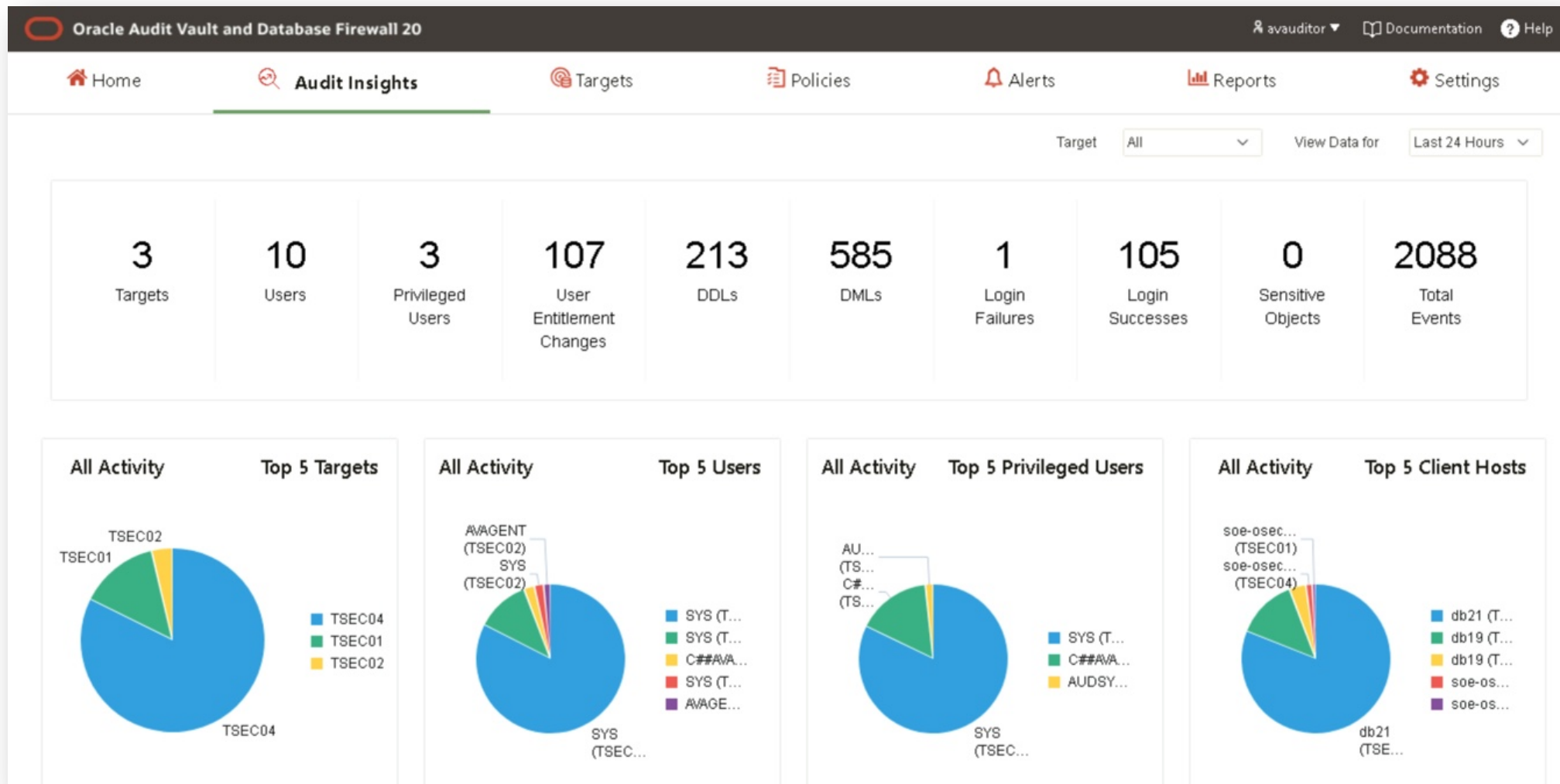
# 3

## Use Cases

Or how AVDF can be used in a meaningful way

# Use Cases

Central Audit Management – one place to store, one view



# Use Cases

## Activity and Compliance Reporting – Predefined Reports

The screenshot displays the Oracle Audit Vault and Database Firewall 20 interface. The top navigation bar includes 'Home', 'Audit Insights', 'Targets', 'Policies', 'Alerts', 'Reports' (highlighted), and 'Settings'. The 'Reports' section is expanded to show 'Activity Reports'. A sidebar on the left lists report categories: Activity Reports, Summary Reports, Compliance Reports, Assessment Reports, Report Templates, Saved Reports, Report Schedules, and Generated Reports. The main content area shows a tree view for 'Activity Reports' with sub-sections: Summary, Data Access & Modification, and Login & Logout Events. The 'Summary' section contains a table of predefined reports.

Report Name	Report Description	Schedule	Generated Report
All Activity	All audited and monitored activity		
All Activity by Privileged Users	All audited and monitored activity by privileged users		

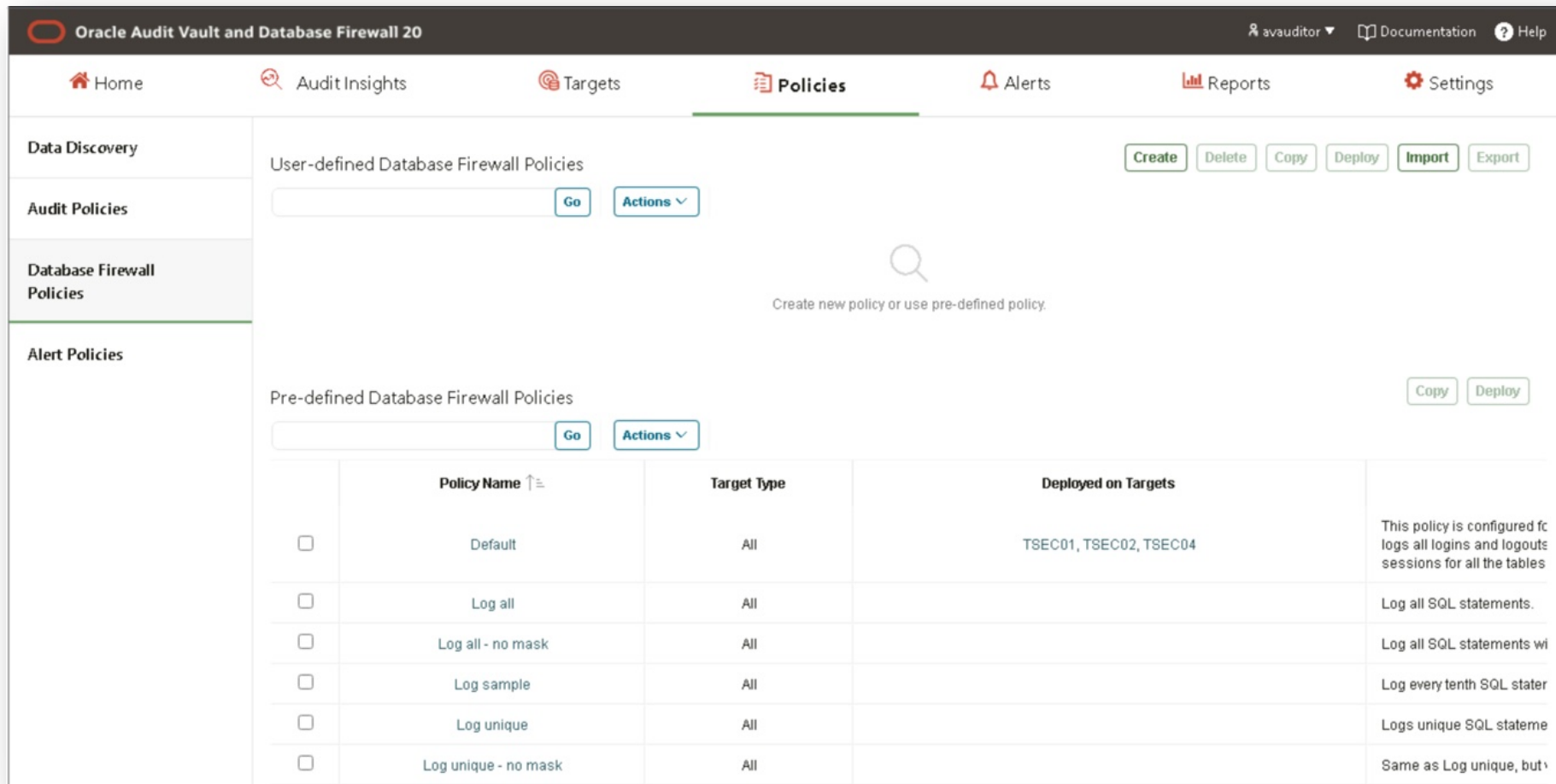
The 'Data Access & Modification' section contains another table of predefined reports.

Report Name	Report Description	Schedule	Generated Report
Data Access	Data access activity (SELECT, Read, etc.)		
Data Modification	Details of Data modification activity (insert, delete, update)		
Data Modification Before-After Values	Before and after values of modified rows in Oracle and Microsoft SQL Server databases		



# Use Cases

## Database Firewall – Place where the real work begins



The screenshot shows the Oracle Audit Vault and Database Firewall 20 interface. The top navigation bar includes Home, Audit Insights, Targets, Policies (selected), Alerts, Reports, and Settings. The left sidebar has Data Discovery, Audit Policies, Database Firewall Policies (selected), and Alert Policies. The main content area is divided into two sections: User-defined Database Firewall Policies and Pre-defined Database Firewall Policies. The Pre-defined section contains a table of policies.

	Policy Name ↑	Target Type	Deployed on Targets	
<input type="checkbox"/>	Default	All	TSEC01, TSEC02, TSEC04	This policy is configured to log all logins and logouts sessions for all the tables
<input type="checkbox"/>	Log all	All		Log all SQL statements.
<input type="checkbox"/>	Log all - no mask	All		Log all SQL statements with
<input type="checkbox"/>	Log sample	All		Log every tenth SQL statement
<input type="checkbox"/>	Log unique	All		Logs unique SQL statements
<input type="checkbox"/>	Log unique - no mask	All		Same as Log unique, but





# Use Cases

## User Entitlement – Monitoring of changes in user, role and rights assignment

Entitlement Reports

Name	Description	Schedule	Gen
Entitlement Activity	Changes in grants of Database privileges and roles		
Privileged Users	Privileged users		
User Accounts	Summary of User accounts		
User Privileges	Summary of User privileges		
User Profiles	Summary of User profiles		
Role Privileges	Summary of Role privileges		
System Privileges	System privileges and their grants to users		
Object Privileges	Object privileges and their grants to users		

User Entitlements

**Last Retrieved** 4/3/2023 3:53:35 PM

**Last Scheduled Run** 4/3/2023 3:53:18 PM

**Next Scheduled Run** 4/4/2023 3:53:18 PM

**Repeats Every** 1 Day

**Retrieve Immediately**

**Create/Update Schedule**



# Use Cases

Store Procedure Audit – Track if, when and by whom changes have been made

Stored Procedure Auditing

**Last Scheduled Run** 4/3/2023 3:53:19 PM

**Next Scheduled Run** 4/4/2023 3:53:19 PM

**Repeats Every** 1 Day

**Create/Update Schedule**

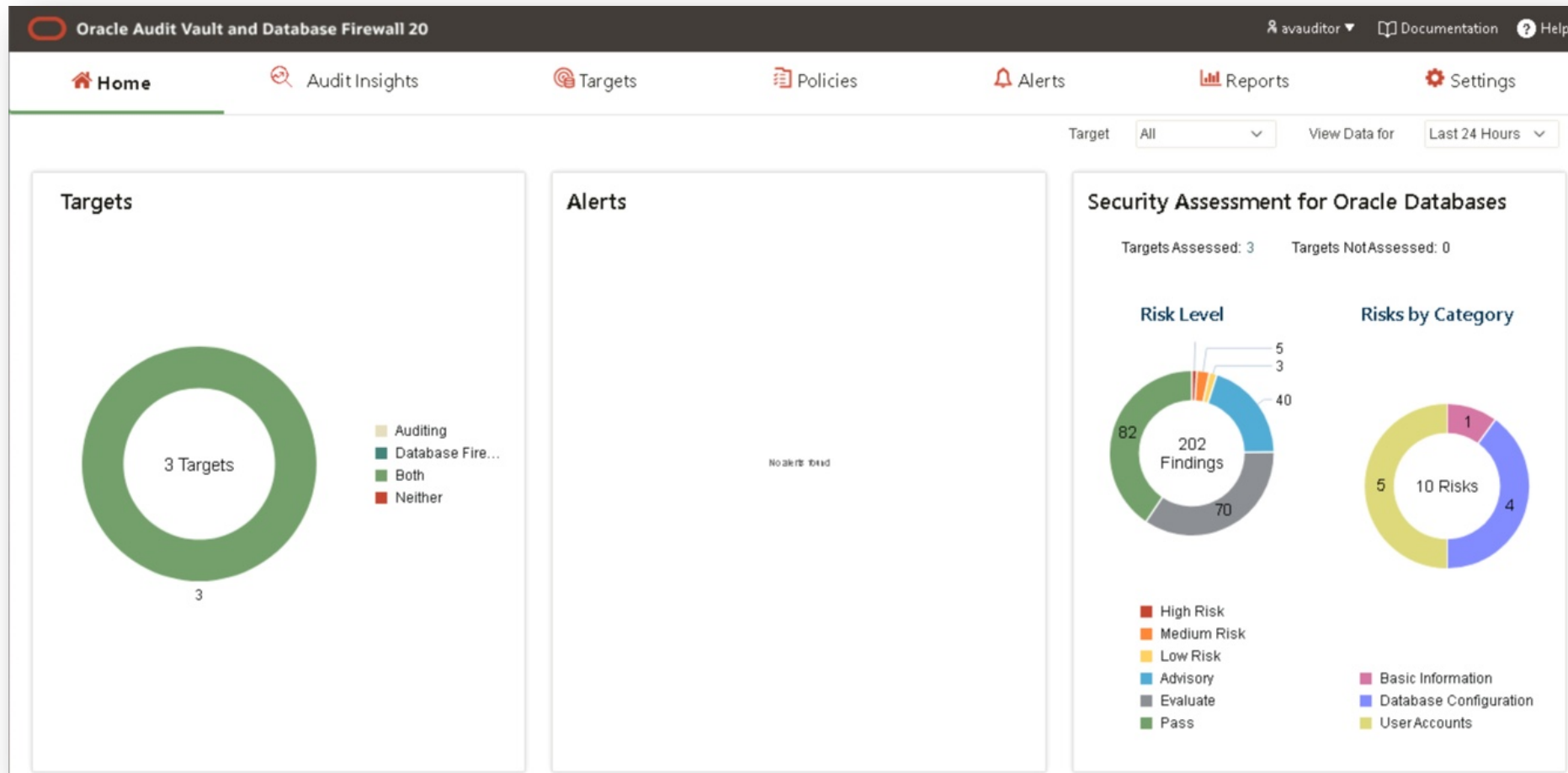
Stored Procedure Changes

Name	Description	Schedule	Generated Report
Created Stored Procedures	Creation history of stored procedures		
Stored Procedure Modification History	Modifications of stored procedures		
Deleted Stored Procedures	Deletion history of stored procedures		



# Use Cases

## Database Security Assessments



# Use Cases

## Privileges Users and Sensitive Object Discovery

The screenshot displays the Oracle Audit Vault and Database Firewall 20 web interface. The top navigation bar includes 'Home', 'Audit Insights', 'Targets', 'Policies' (selected), 'Alerts', 'Reports', and 'Settings'. The left sidebar contains 'Data Discovery', 'Audit Policies', 'Database Firewall Policies', and 'Alert Policies'. The main content area is titled 'Policies' and contains the following text:

Discover privilege users using User Entitlements and sensitive objects using DBSAT reports in your databases to enable creation of appropriate sets. Later use them in Database Firewall policies.

To configure User Entitlements and Sensitive Objects jobs, click on the "Schedule Retrieval Jobs" icon for a given target. Please refer to [Schedule Retrieval](#)

These sets are also available for policy creation using the "User-defined Database Firewall Policies" workflow.

**Privileged User Sets (1)**

Discover privileged users using User Entitlements in your databases. A privileged user set can be created from the list presented, and one can add or remove users as per the choice. These sets can later be used in other policies or rules.

**Add** **Delete**

<input type="checkbox"/>	Name ↑	Values	Description
<input type="checkbox"/>	PUSet01	APPQOSSYS,AUDSYS,C##AVAGENT,DBSNMP,GSMADMIN_INTERNAL,GSMCATUSER,GSMUSER,SYS,SYS\$UMF,SYSBACKUP,SYSDBG,...	Privileged User Set 01

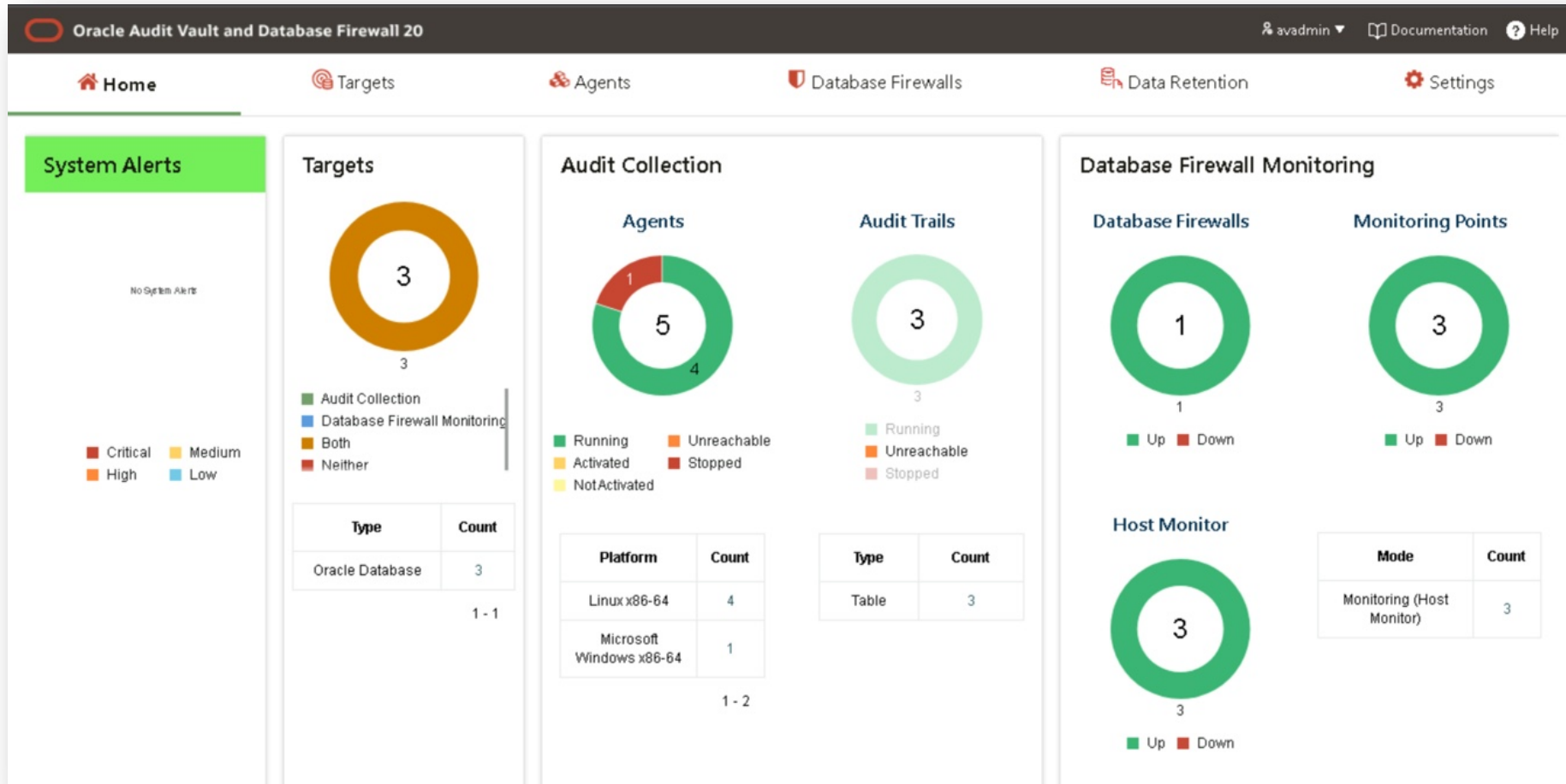
1 - 1

**Sensitive Object Sets (0)**

**Database Firewall Policies (0)**

# Use Cases

AVDF Infrastructure Administration – Archiving, High Availability, and more...



# 4

## **Latest Enhancements**

Oracle AVDF 20.9 and  
earlier

# Releases Support Notes

## General Notes about Oracle AVDF enhancements

New versions of AVDF are released on a regular basis

- Released about **twice a year** see Oracle Support Document [1328209.1](#)
  - AVDF Release Update 7 (RU7) June 2022
  - AVDF Release Update 8 (RU8) September 2022
  - AVDF Release Update 9 (RU9) March 2023
- **Release Update** includes...
  - critical functional and security fixes e.g. Oracle Critical Patch Updates for the whole stack
  - New features and enhancements
- Covers all components e.g. **Audit Vault** and **Database Firewall**

**It is recommendet to stay up to date...**



# Latest Enhancements

## Oracle AVDF Release 20.9

- **Security Assessment** centralized security assessment solution for enterprises by integrating the popular Database Security Assessment Tool (DBSAT)
- **Discover sensitive objects and privileged users** AVDF 20.9 now helps customers discover sensitive data and privileged users in the Oracle database
- **Audit Insights** Customers can now get immediate insight into the top user activities across one or multiple databases
- **Before/After reporting for Microsoft SQL Server** The Before/After report for the Microsoft SQL server is a valuable addition to the already available before/after report for the Oracle database, helping organizations improve their compliance posture
- **Data Retention** Administrators can streamline data retention with a simplified lifecycle management process and a target-focused view





# Latest Enhancements

## Oracle AVDF Release 20.9

- **Agentless Audit Collection** It is now possible to accelerate the deployment of AVDF with the agentless audit collection service for Oracle databases. There's no need for agent installation or upgrades on target Oracle databases. Ideal for small or remote deployments and proof of concepts.
- **System Alerts** Administrators can now be alerted on the status of critical AVDF changes, such as high availability configuration, storage availability, certificate expiration, and password expiration.
- **Out-of-Place Upgrade** Increase system availability during updates and upgrades with minimal downtime, typically in minutes.
- **Upgraded Platform** The operating system for the Oracle Audit Vault Server and Database Firewall Server has been updated to Oracle Linux 8.



# 5

## Best Practice

Tips on how to avoid  
common mistakes

# Oracle Audit Concept

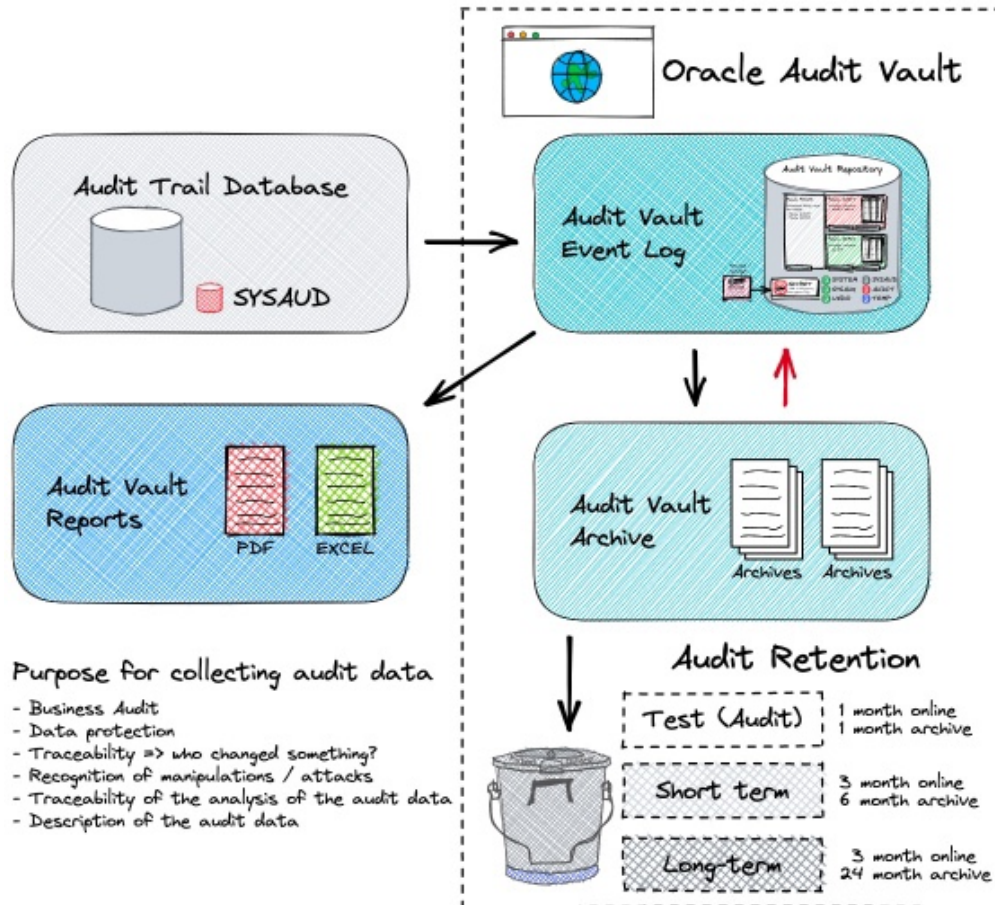
Comprehensive audit concept independent of AVDF



**It is essential that you  
have your audit settled  
before deploying AVDF**

# Data Retention

Keep the beast in check!



**Audit Trail:** decentral source of audit data

- Storage requirements on source system, relatively cost intensive, risk of data tampering, no overall analysis

**Audit Vault Event Log:** central online storage of audit data

- Detailed central audit information, overall analysis, Appliance size sets storage limits

**Audit Vault Archives:** offline storage of audit data

- Offline archive freeing storage on Audit Vault server, must be brought back online for analysis

**Audit Vault Reports:** summarized audit informations

- consolidated information, low memory requirements, long-term storage possible

The retention period of audit data determines storage needs

**Choose wisely  
where to store data and  
for how long**

# Sizing

As much as necessary not as much as possible...

Driver for Audit Vault and Firewall Sizing

- **Audit Policies / Trails**

- Type of audit trails
- Size of audit records
- Number of audit trails

- **Retention** period of the data

- What and how long
- Business and compliance needs

Oracle Calculation Guideline

- Simple **excel spreadsheet** to calculate requirements for *Audit Vault Server, Audit Vault Agents, Database Firewall* storage, CPU and memory requirements
- Oracle Support Document [2092683.1](https://support.oracle.com/defectdetail?defect_id=2092683.1)

Oracle Audit Vault and Database Firewall Sizing Guide (version 2.5)							
Calculator provides system sizing guidance for: Audit Vault Server (AVS), Audit Vault Agent (AV Agent) and Database Firewall (DBFW) <a href="#">. See Column A for what information to fill.</a> Note: Refer to the sheet "AVS Database Parameters" to check if any changes are needed to the AVS database parameters.							
Inputs for Audit Vault Server Sizing							
Audit Category	Number of Audit targets	Average Audit Records per day per target	Average Audit Record size (bytes)	Audit Retention Period (Days)	Total Audit Records per day from all targets	Daily Volume of audit data (GB)	Total Required Storage (GB)
Low	10	500	1'500	90	5'000	0	3
Medium	15	5'000	1'500	90	75'000	0	46
High	5	25'000	1'500	90	125'000	0	76
Extreme		125'000	1'500	90	0	0	0
Custom1			1'500	90	0	0	0
Custom2			1'500	90	0	0	0
Custom3			1'500	90	0	0	0
DB Firewall Log Category	Number of DBFW targets	Average number of statements logged per day per target	Average Log Record size (bytes)	Log Retention Period (Days)	Total logged Records per day from all targets	Daily Volume of log data (GB)	Total Required Storage (GB)
Low	0	5'000	1'500	90	0	0	0
Medium	2	50'000	1'500	90	200'000	0	25
High	10	250'000	1'500	90	5'000'000	7	629
Extreme	100	1'250'000	1'500	90	250'000'000	349	31'433
Custom1		25'000'000	1'500	90	0	0	0
Custom2			1'500	90	0	0	0
Custom3			1'500	90	0	0	0
					2953.703704		

**In-Memory Usage**  
1. How many months data will you keep in memory? (optional, needed only if using the in-memory feature. Default=0)

**Audit Vault Server Sizing Recommendation**

AV Server Storage Requirements (GB): (300GB out of this must be on local disk(s))	96937
Recommended memory (GB) for In-Memory option	0
AV Server Memory Requirements (GB)	159
AV Server CPU Requirements:	10

**Input:** Enter values in columns C-F. Columns D-E, F are pre-populated, but can be changed. Column B represents the Target Audit Category for the AV Server or the DB Firewall:

**Low** = minimal data being captured and retained by audit/firewall policies--> For example - auditing only the failed logins, firewalls set to log none by default with few exceptions  
**Medium** = typical data collection--> For example - Low Audit + auditing privileged user activities, auditing failed/successful logins  
**High** = deeper audit, collecting data for systems with a stronger need for reporting and analysis; --> For example - Medium Audit + privilege changes (DCLs) and metadata changes (DDLs)  
**Extreme** = very high volume systems when anomaly detection is required; tracking of data access, etc--> For example - High Audit + auditing access to tables

For higher numbers than the Extreme Audit please use the "Custom" rows. Columns G, H, I should not be changed as they are computed.  
**Note:** When new rows are added under Custom options, make sure the formulas for cells G-I are updated. Also, ensure that the formulas for "AV Server Storage Requirements" and "AV Server CPU Requirements" cells are updated.

A CPU is defined as one CPU core. Equivalent to a single OCPU and usually equivalent to two vCPUs

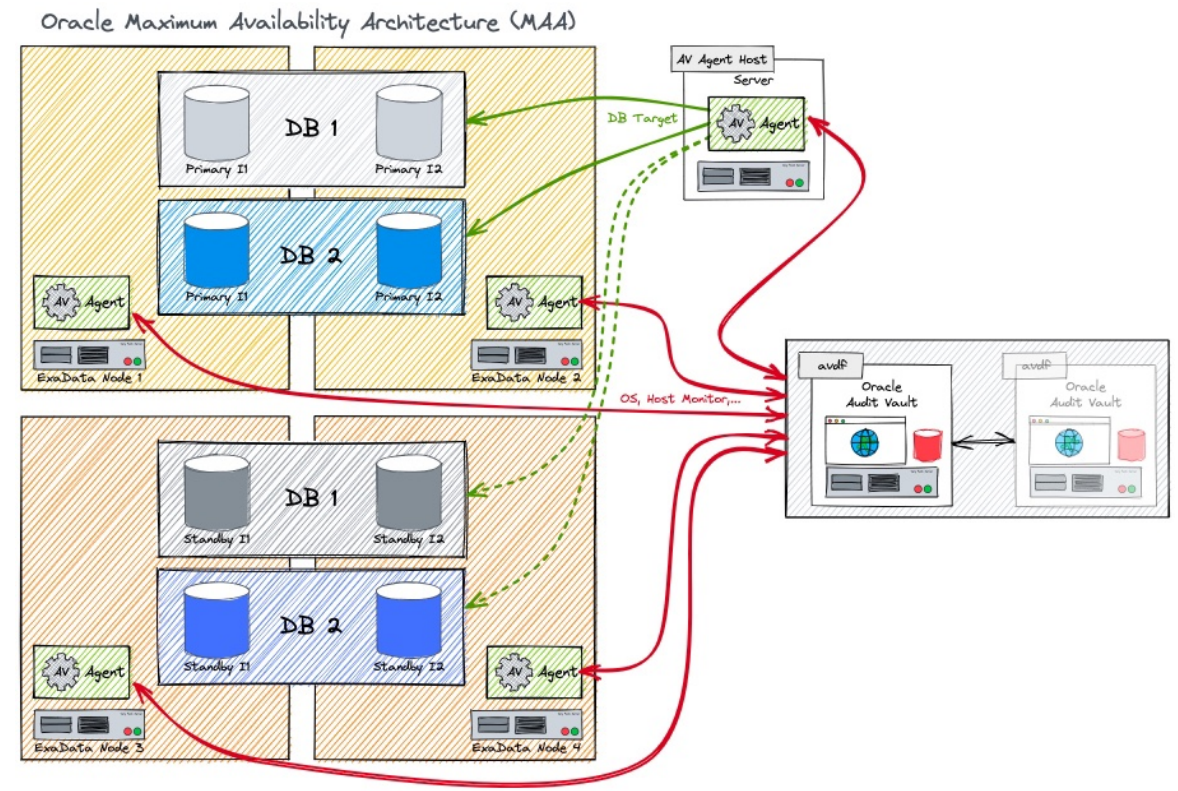


# High Availability

## Oracle AVDF versus Audit Trails

What must be high available?

- **Audit Vault Server** in High Availability Mode
  - Two AV Server paired for business continuity
  - Configured internally as Standby Database
- **Audit Vault Agent**
  - Configured as cluster resource
  - Single point of failure
  - Local buffer in audit trails
- **Audit Trail**
  - Depends on trail type e.g. Database, OS, RAC, DataGuard,...
  - Will keep audit data until it is processed





**Is it necessary to keep all  
components  
high available?**

# 6

## Licensing

How much does it cost?

# Licensing

## Licensing model for Oracle Audit Vault and Database Firewall

**One License** to rule them all. i.h., Oracle AVDF license covers

- *Audit Vault Server and Database Firewall*
- *Audit Vault Agents with plug-ins as well Host Monitor*
- *Enterprise Manager plug-in for Oracle Audit Vault and Database Firewall*
- Special-Use licensing covers also all stacked software application

**Licensing** for *Oracle Audit Vault and Database Firewall* is based on:

- The targets being monitored
- The number of processors on the computers where the targets are located
- The number of named users of those targets

**Unrestricted use could become expensive**



# 7

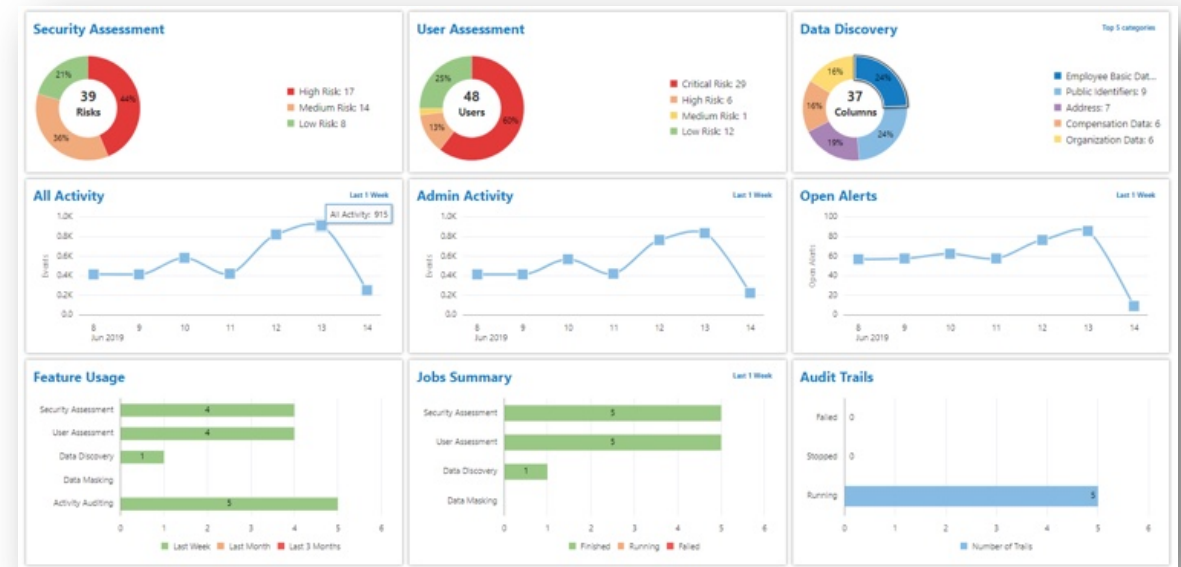
## Other Solutions

Alternative Solutions  
and Products

# Oracle Data Safe

## Cloud based Database Security Service

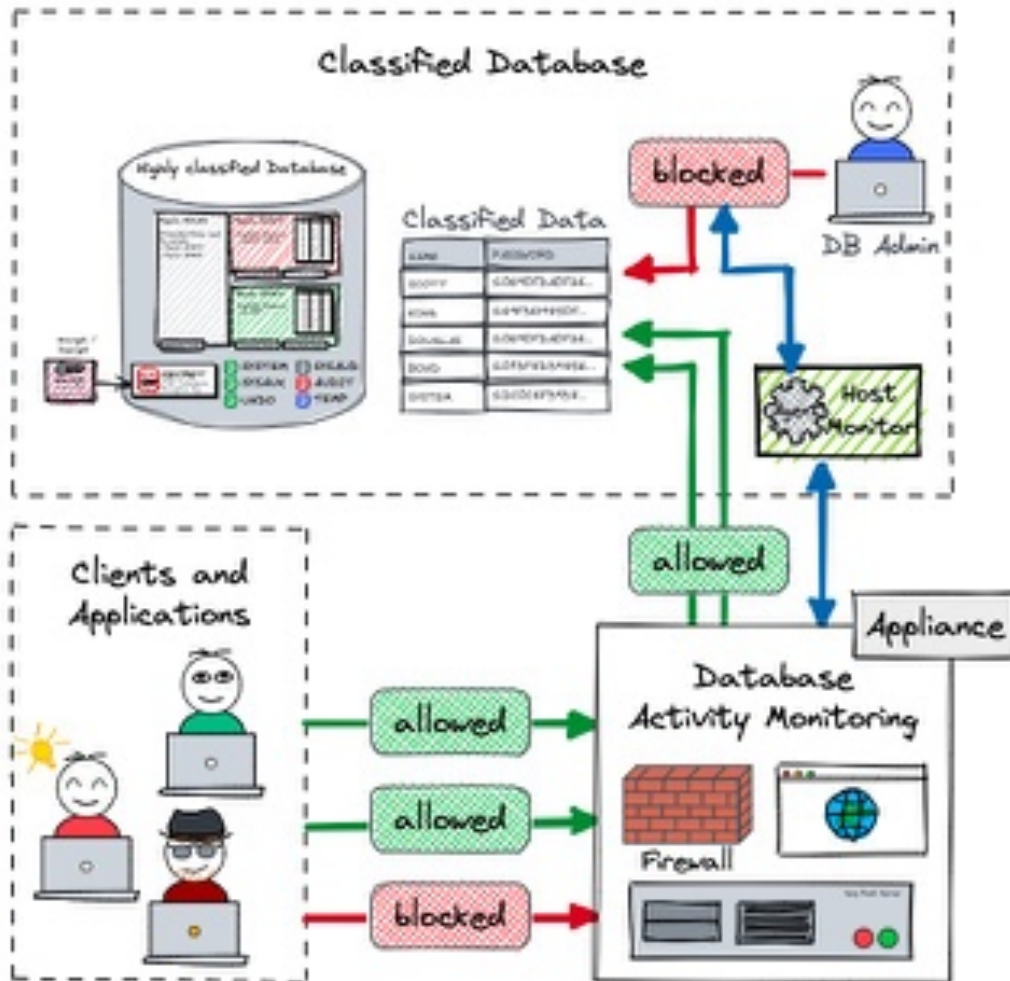
- **Security Assessment** to assess the security of database configurations
- **User Assessment** to assess the security of database users and identify high risk users
- **Data Discovery** to identify sensitive data in databases
- **Data Masking** provides a way to mask sensitive data so that the data 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 ...

# Custom Solutions

What ever you like to build...

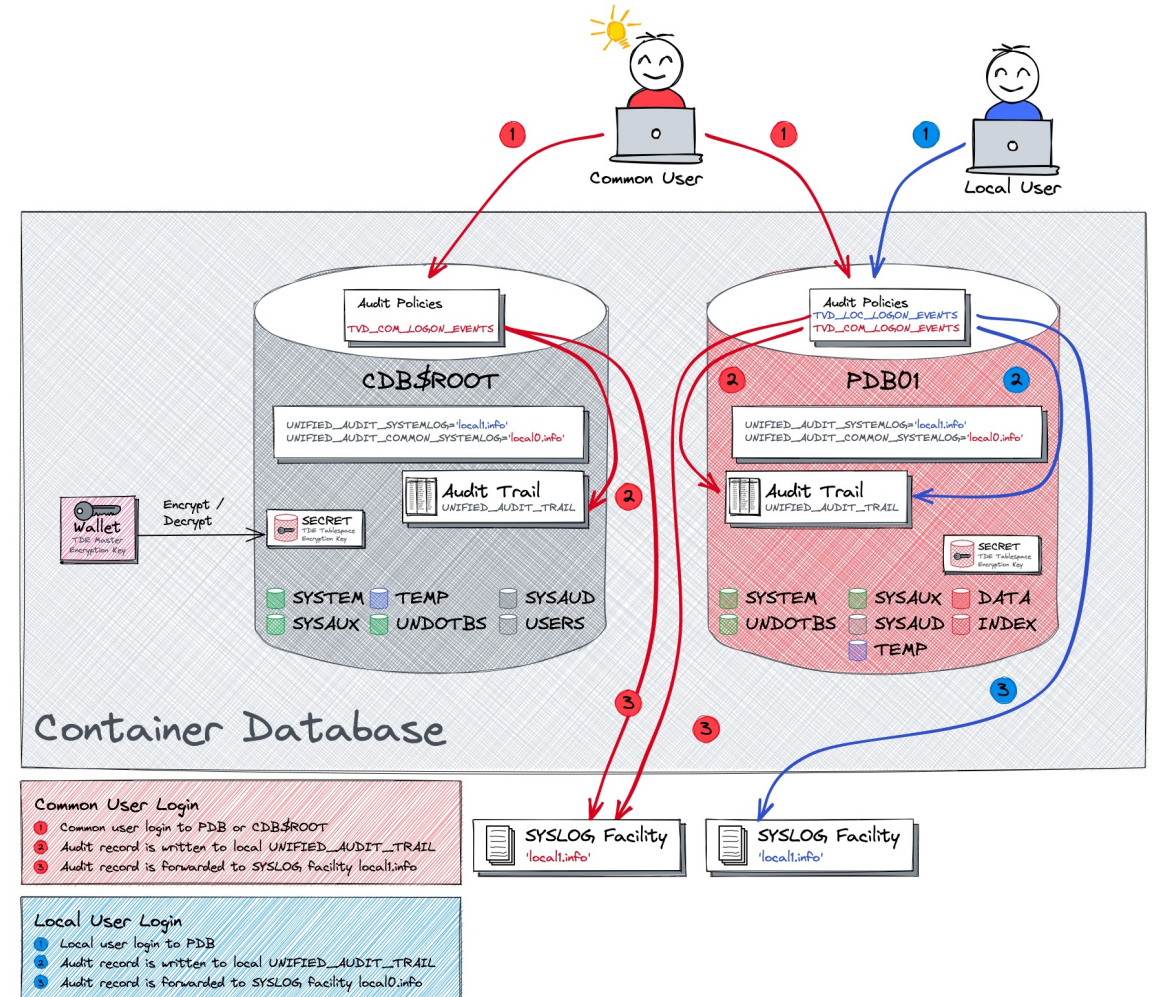
The solutions are usually **limited** to...

- 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



# 8

## Conclusion

Is AVDF a Product for  
your Database  
Environment?



# Conclusion

## Is AVDF a Product for your Database Environment?

- Oracle Audit Vault and Database Firewall has **grown up**
- Regular **release updates** as of major release Oracle AVDF 20

Two major **challenges** remain:

- **Operation** of a software appliance
  - Perfect for none DBA based operation
  - Not everything is reasonable/possible
- (Storage) **Space**: the final frontier
  - **too much** audit data makes handling sluggish
  - **SAN / iSCSI repository** extends the storage boundaries
  - Appropriate **retention intervals** are a prerequisite

## 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



**The main challenge is  
still the security concept  
of the databases.**

**Thank You**



# Oracle AVDF Sources

Documentation, White Papers, Support Notes and other Links

- Oracle Audit Vault and Database Firewall [online documentation](#)
- Oracle Database Unified Audit [Best Practice Guidelines](#)
- [1681969.2](#) Oracle Audit Vault and Database Firewall
- [1328209.1](#) Oracle AVDF (Audit Vault and Database Firewall) Releases Support Status
- [2092683.1](#) Audit Vault and Database Firewall Best Practices and Sizing Calculator for AVDF 12.2 and AVDF 20
- [2725072.1](#) How to Deploy Audit Vault & Database Firewall (AVDF) In OCI?

