Oracle Database Security

But what about performance?

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)

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

Agenda

Or how best to burn down time in your spare time…

1. Motivation
2. Security vs Performance?
3. SQLNet and Authentication
4. SecBench and SwingBench
5. TDE Use Cases
6. General Use Cases
7. What's Next?
8. Conclusion

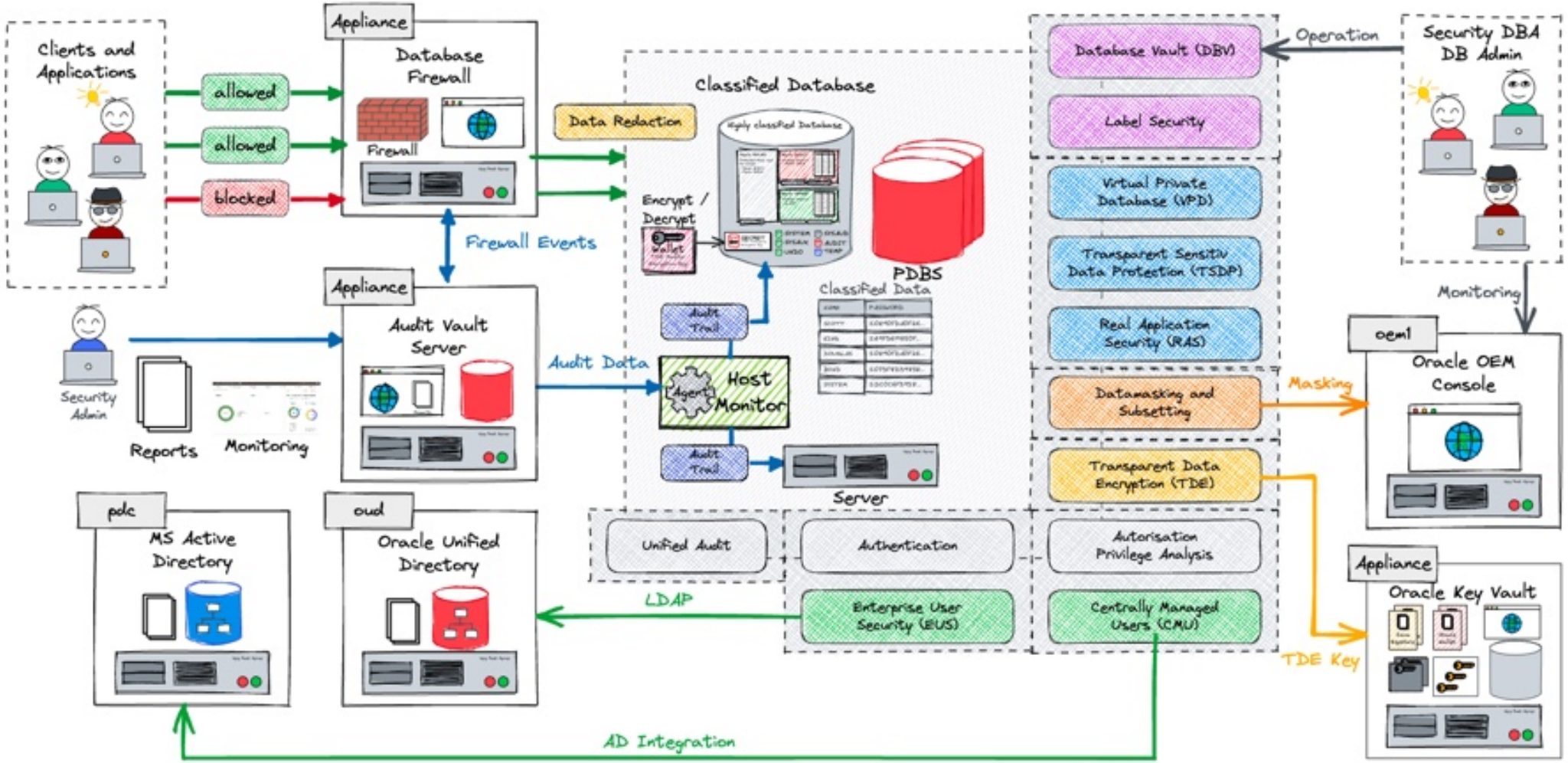
1

Motivation

Why did I start this topic in the first place?

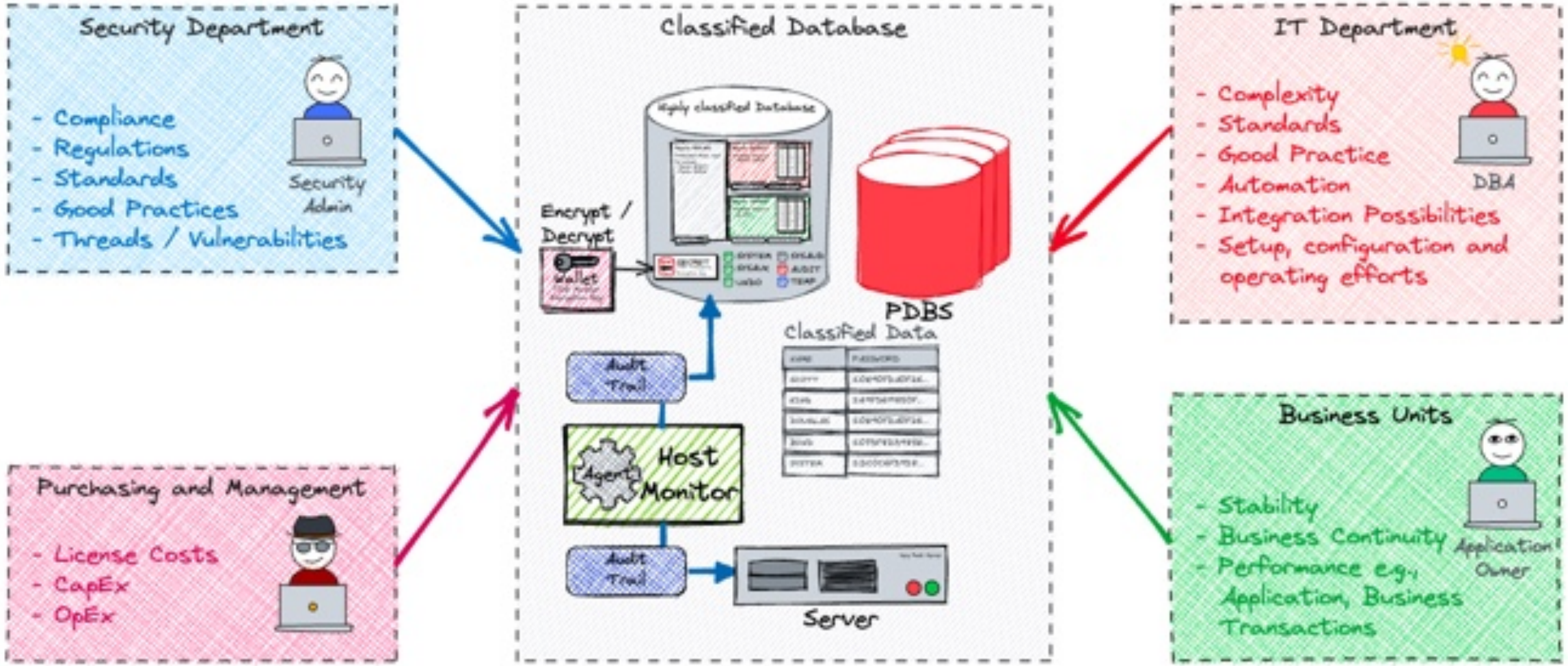
Oracle Database Maximum Security Architecture

All Oracle Security Features and Options at a glance



Various Stakeholder

Everyone has their requirements for database security



Where to start, where to stop?

My journey has been a bit bumpy so far

- Select a **suitable environment**. Cloud or rather on-premises?
- Choosing **tools** for capturing and measuring **key performance indicators**
- Definition of appropriate **security configurations** and **use cases**
- Define baselines
- Create a suitable **workload**
- **Scripting** and **automating** the bloody thing
- Initiate use case, wait, fix problems and start again (and again,...)
- Describe a framework which can be used to reproduce use cases / workload between different environments and releases.

To be honest that is still going on

Charlie Chaplin in Modern Times (1936). © Roy Export Company Establishment; photograph, the Museum of Modern Art/Film Stills Archive, New York City

Research, Engineering or Development?

I overestimated the effort a bit and I'm still not where I want to be....

```
soe@host:~/github/oehrlis/ > cloc secbench
      149 text files.
      88 unique files.
      63 files ignored.
github.com/AlDanial/cloc v 1.96  T=0.12 s (719.4 files/s, 49774.4 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Bourne Shell                    26            422            946           2164
SQL                             34            186            763           1054
Markdown                        23             97              4            277
YAML                             1             12             48             54
Bourne Again Shell               1              5             26             28
Text                             3              0              0              3
-------------------------------------------------------------------------------
SUM:                            88            722           1787           3580
-------------------------------------------------------------------------------
```

2

Security vs Performance?

Why and where is performance relevant for database security?

Performance

What is relevant for an environment?

- There are different aspects of performance
  - Many of them **depend on each** other
- Application owner is primarily interested in **business processes** rather than theoretical benchmarks

An example:

- From a business point of view, the **pure hardware performance** metrics are not necessarily important
- One is more interested in **how long** the business process **takes**.
  - e.g. how many orders are executed per minute, does the analysis take 30 minutes or rather 4 hours?
  - The read/archive performance of an audit trail can be irrelevant whereas a write access to the audit trail has an impact on the business performance
  - Logon time is irrelevant when data processing takes hours

Performance

There is no conclusively correct answer....

- It is important to **know the business requirements** in advance.
- Implementing security measures on a **critical system** will always have a negative impact.
  - It did work before...
  - Since you enable xyz my report run's slower
- It is advisable if you **know your system** / application
  - It is recommended to have reproducible tests e.g. simple scripts or better full regression tests
  - Consider stuff like *Oracle Real Application Testing*
- Be prepared to prove impact of changes

3

SQLNet and Authentication

Or what happens when you change SQLNet and authentication....

Use Case SQL Net Logon Times

The idee behind this is a customer application

- A customer start to use **strong** and **central** database authentication across its environment
  - *Oracle Kerberos Authentication* with *Oracle Centrally Managed Users (CMU)*
- Some applications are quite **sensitive** to changes in connection establishment
  - Many but relatively short connection times e.g. a couple of milliseconds
  - It is relevant if a logon times 50ms or 250ms
- **Simple tests** were performed to establish the connection:
  - The test includes 1000 connections samples.
  - Time measurement is done with the help of the *SQLNet* trace file and network tracing
  - The **absolute connection** times contain the actual **network activity** as well as everything that is necessary to establish the connection, i.e. the exchange of keys etc.

SQL Net Test Cases

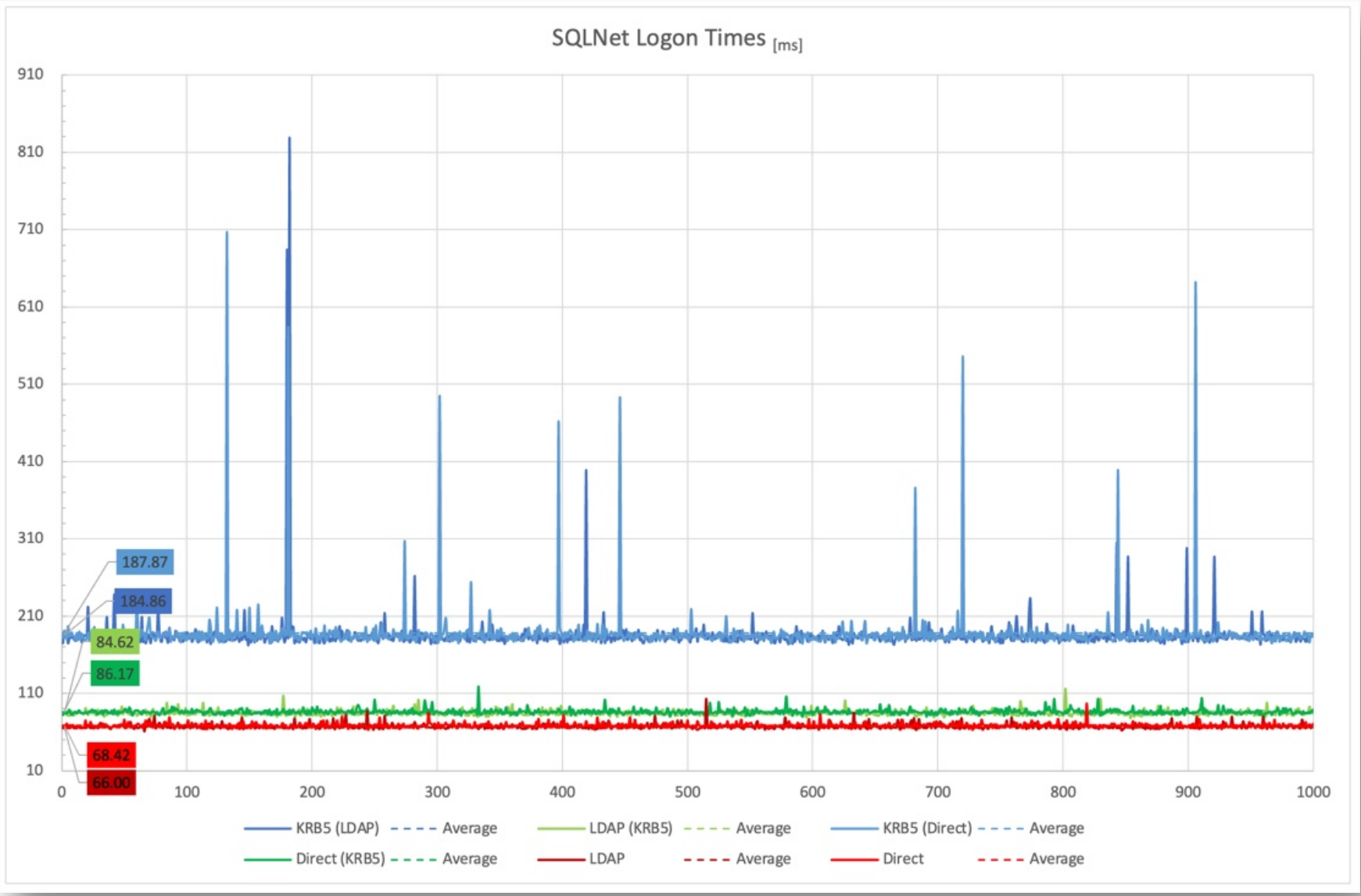
What did we test…

The following connection tests are made for this purpose:

- **KRB5 (LDAP)** Kerberos with LDAP Oracle names resolution
- **KRB5 (Direct)** Kerberos authentication with direct connect
- **LDAP (KRB5)** Password authentication with LDAP Oracle names resolution and Kerberos configured in *SQLNet* but not used
- **Direct (KRB5)** Password authentication with direct connect and Kerberos configured in *SQLNet* but not used
- **LDAP** Password authentication with LDAP Oracle Name resolution.
- **Direct** Password authentication with direct connect.

Inaccuracies due to network caching etc. are likely and cannot be explicitly excluded

SQL Net Logon Times



Some conclusions

Is this now an Issue?

- Remote logins usually take about 10ms longer than local connections.
- All connect with *tnsnames.ora* lookup are slightly faster.
- Kerberos based logons are slower due to the extra roundtrip to the KDC i.e. 170-190ms
- Kerberos based logons are more likely to have peaks.
- Regular DB logon are faster but around 15ms slower if the DB server is permanently configured with Kerberos.

Conclusion

- *SQLNet* with Kerberos has an impact on logon time. This is true for both Kerberos and Password authentication.
- The effect is relatively small with an average of 70ms
- Other SQLNet configurations like network encryption, check summing or similar have much higher impact on the login time.

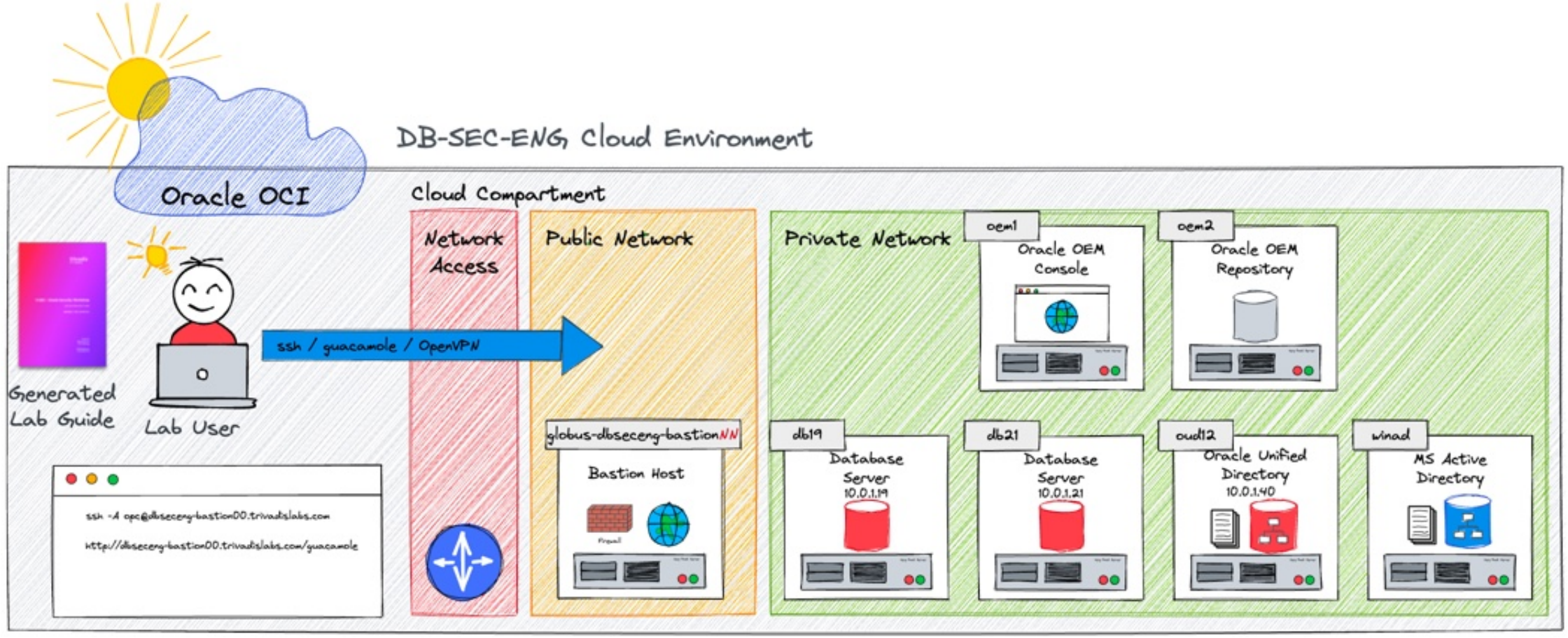
4

SecBench and SwingBench

Selected toolset and lab environment

Lab Environment

OCI based Lab… happy terraforming

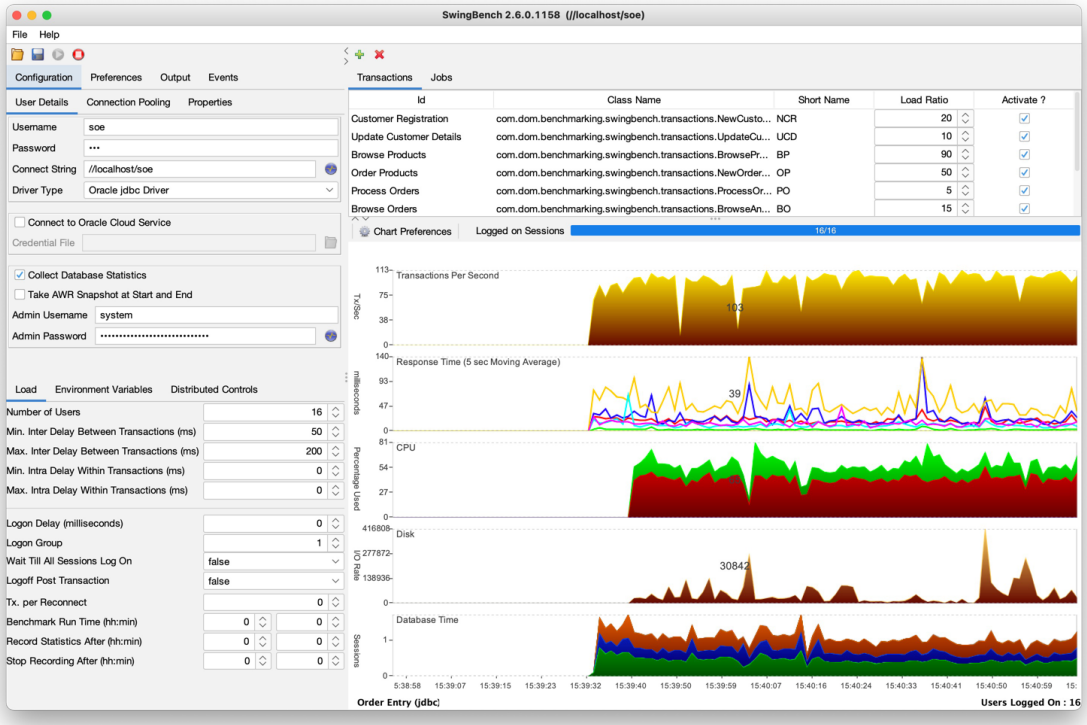


SwingBench

A tool to stress your Oracle Databases

- **Swingbench** is a load generator and associated set of utilities
  - Preparation of test data / schemas
  - Run and monitor load tests
  - Analysis of results
- Designed for stress testing various Oracle database releases
  - Currently 12c, 18c, 19c, 21c, 23c
- A comprehensive set of predefined workloads is provided
  - E.g. OrderEntry, SalesHistory, TPC-DS Like, TPC-H Like, JSON, Movie Stream and StressTest
- Java based
- Developed and maintained by Dominic Giles
  - Oracle Database Product Manager

See also https://www.dominicgiles.com/index.html



SecBench

One toolset emerged in the need

- *Swingbench* tests usualy do **run** for a **while**
- Security use cases do **require** some **configuration** e.g. enable DBV, set audit policies etc
- It is always necessary to create a defined starting position
  - E.g. see blog post by Dominic Should I Restore The Database After Each Benchmark Run?

Solution approach of SecBench

- Use of a container database
- Initially create a SecBench **seed database**
  - required configuration, database options, tablespaces, Swingbench schema etc.
- **Clone** the seed database for each benchmark respectively security use case
- **Configure** security use case in PDB e.g. enable TDE, Audit etc.
- See https://github.com/oehrlis/secbench

Grafana and Prometheus

A perfect couple for simple host monitoring

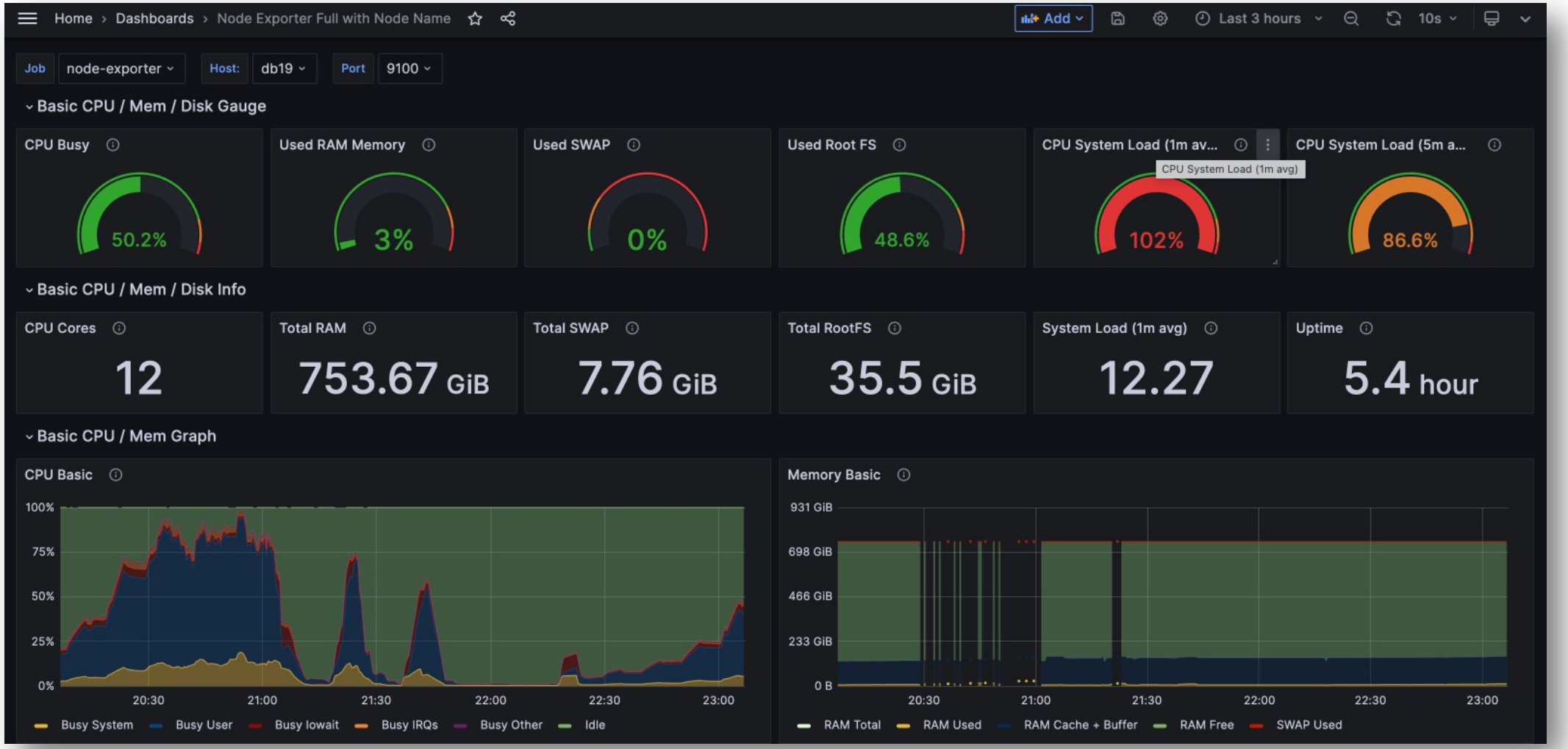
- Oracle and Swingbench provide a lot of information:
  - Performance details create using AWR snapshots
  - Swingbench does collect information like transaction times e.g. TPS, TPM, Response times etc.
- However, there is a need to collect information on the system/hardware resources

Solution approach

- Docker based Setup using Grafana and Prometheus
- Prometheus node explorer to collect system information
- Setup done in a couple of minutes
- Run’s on my bastion host in the cloud environment
- Simple way to compare if more or less OS resources are used

Dashboard

Simple Dashboard based for Node Explorer



5

TDE Use Cases

In search of the Achilles heel of TDE...

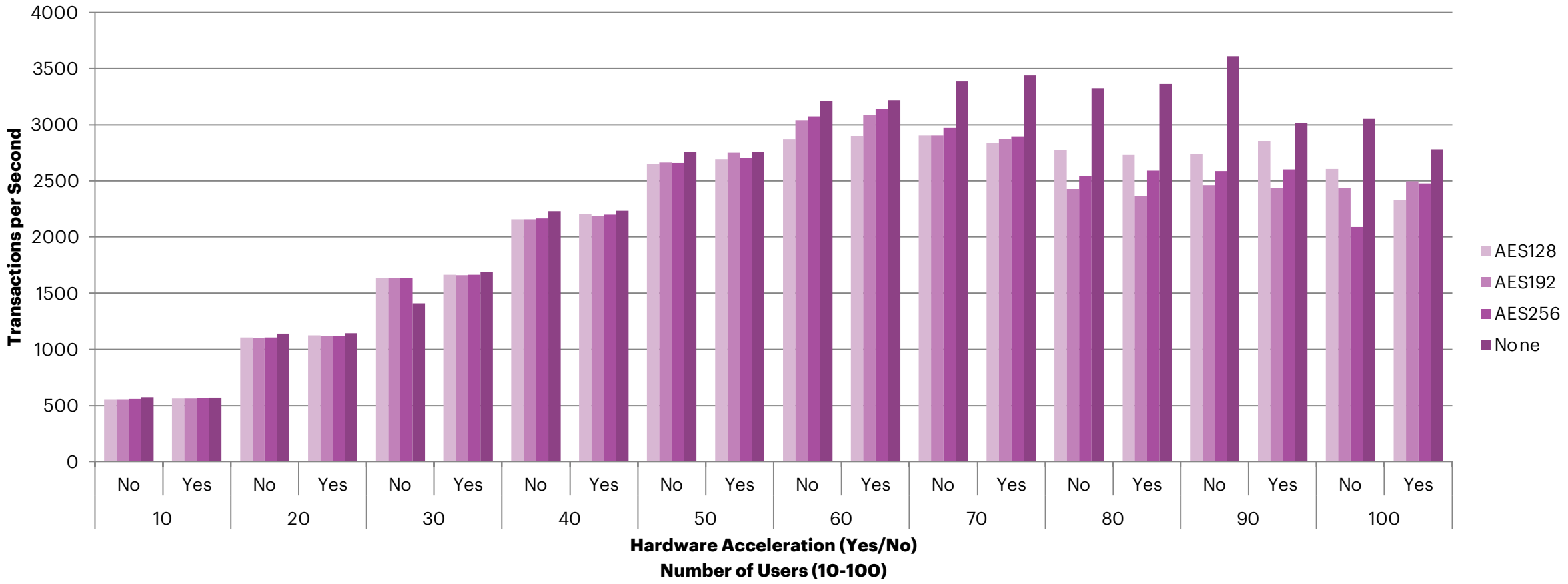
Performance Test

Not quite recent tests with Oracle 12...

- Swingbench tests with Oracle OrderEntry schema (OE) and runtime parameters
- Scale: 50, All indexes, No partitioning
- Configuration of the tests :
  - Runtime: 30 minutes, min/max intra transaction think time: 1/6
  - Number of users: 10,20,...,90,100
- Measured values
  - Number of transactions per second (TX per sec)
  - CPU time used

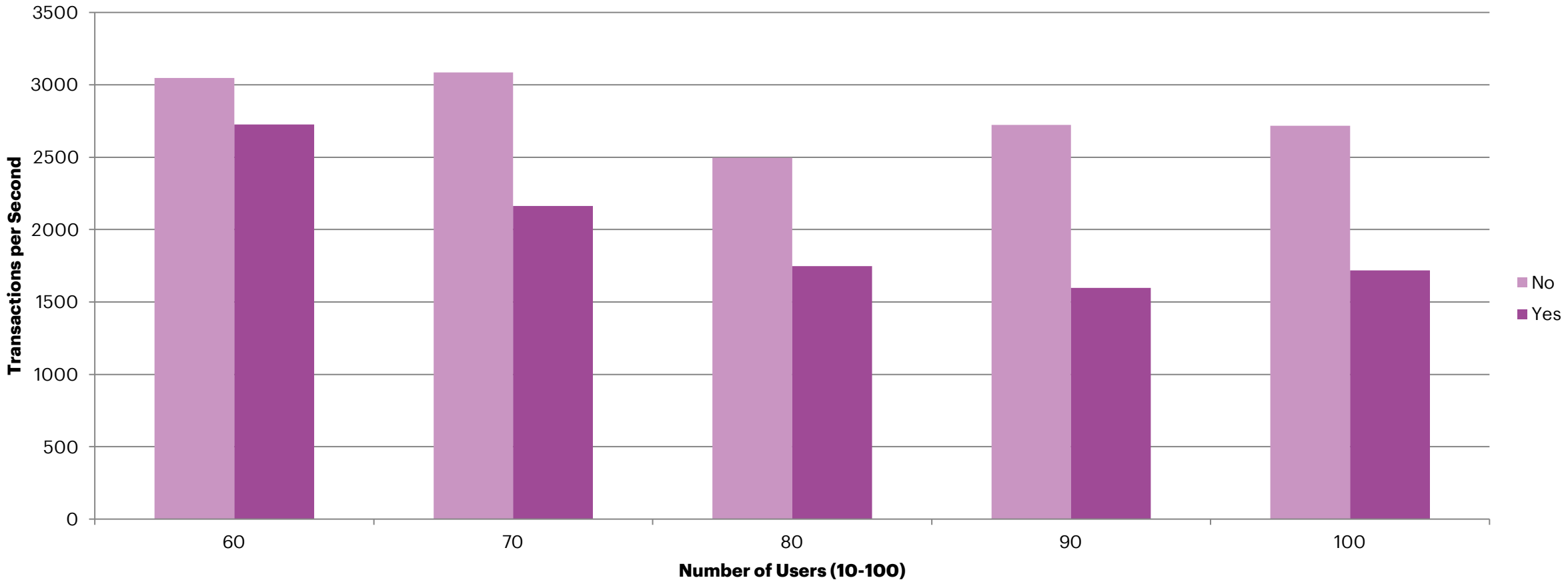
Performance Test Results

Transactions per second for 10,...90,100 users with and without AES-NI library.



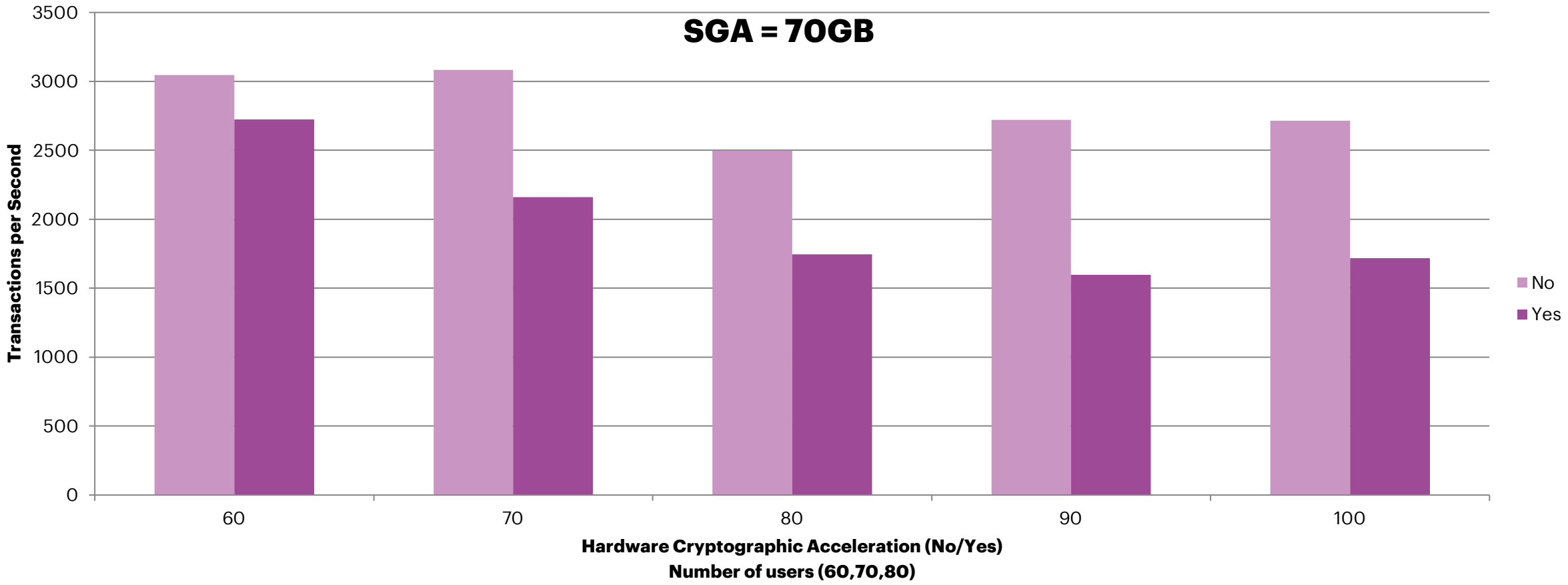
Performance Test Results

Average transactions per sec for encrypted / unencrypted tablespaces



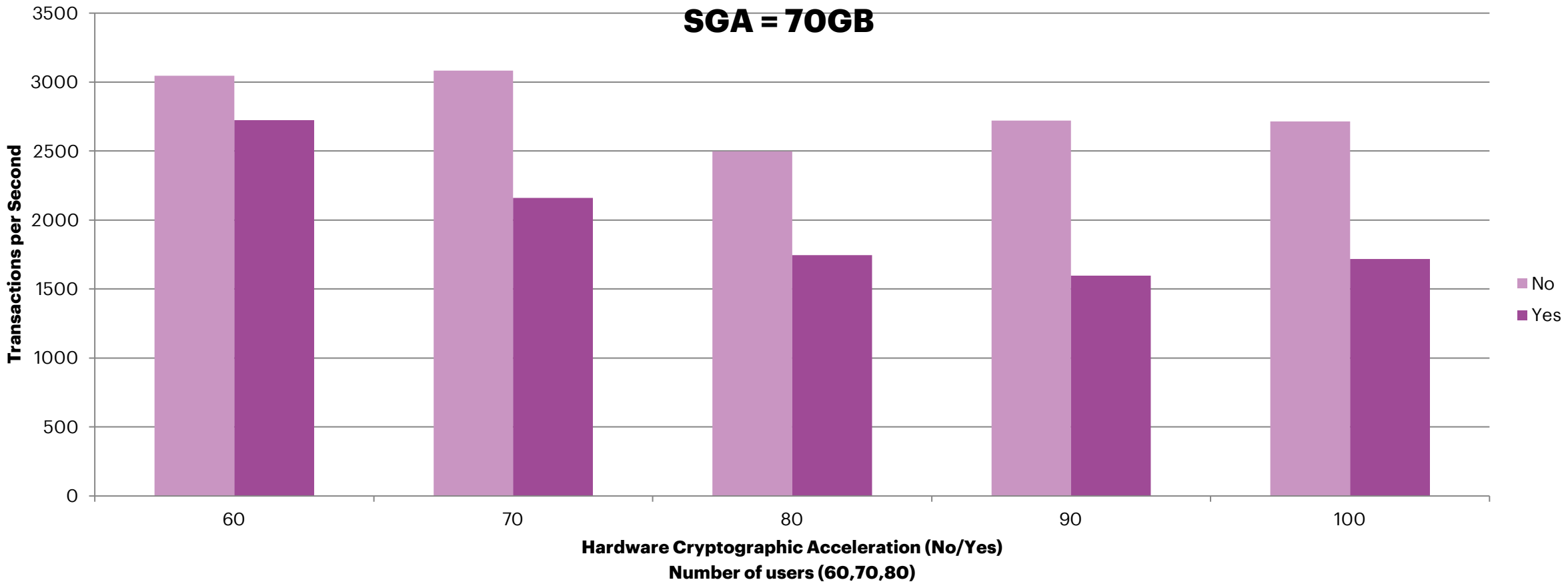
Performance Test Results

Transactions per second for 7GB SGA



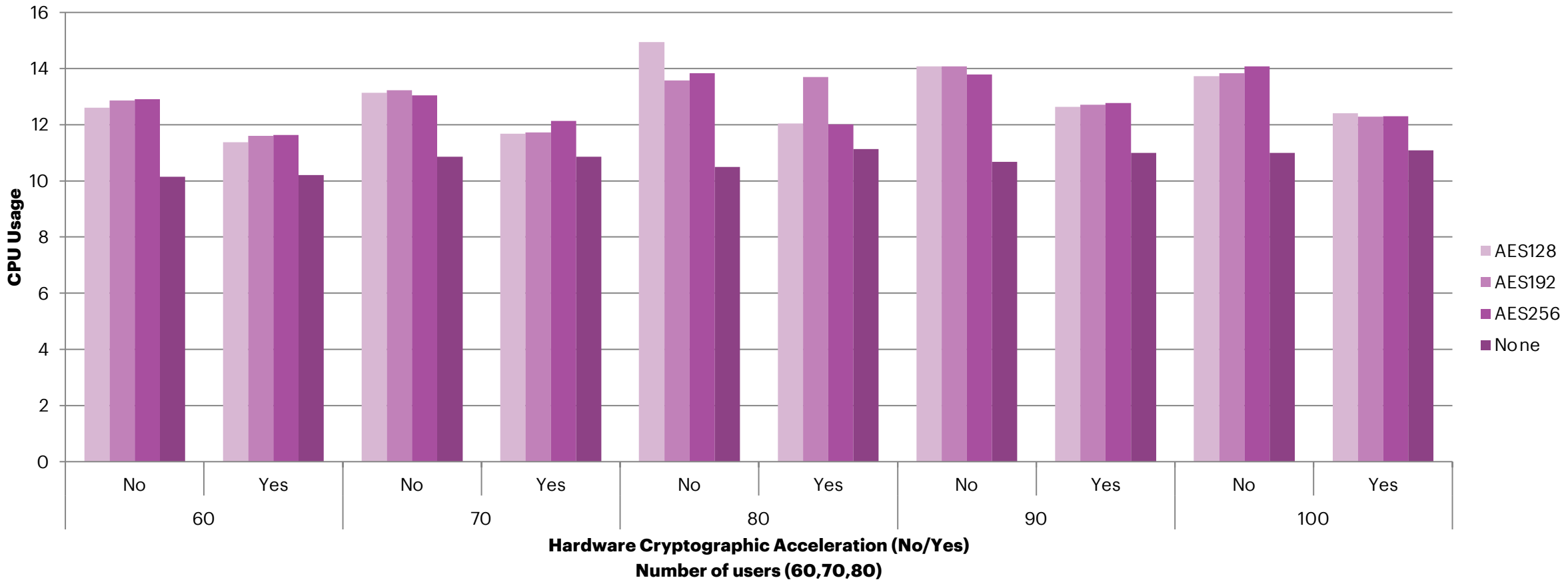
Performance Test Results

Transactions per second for 70GB SGA



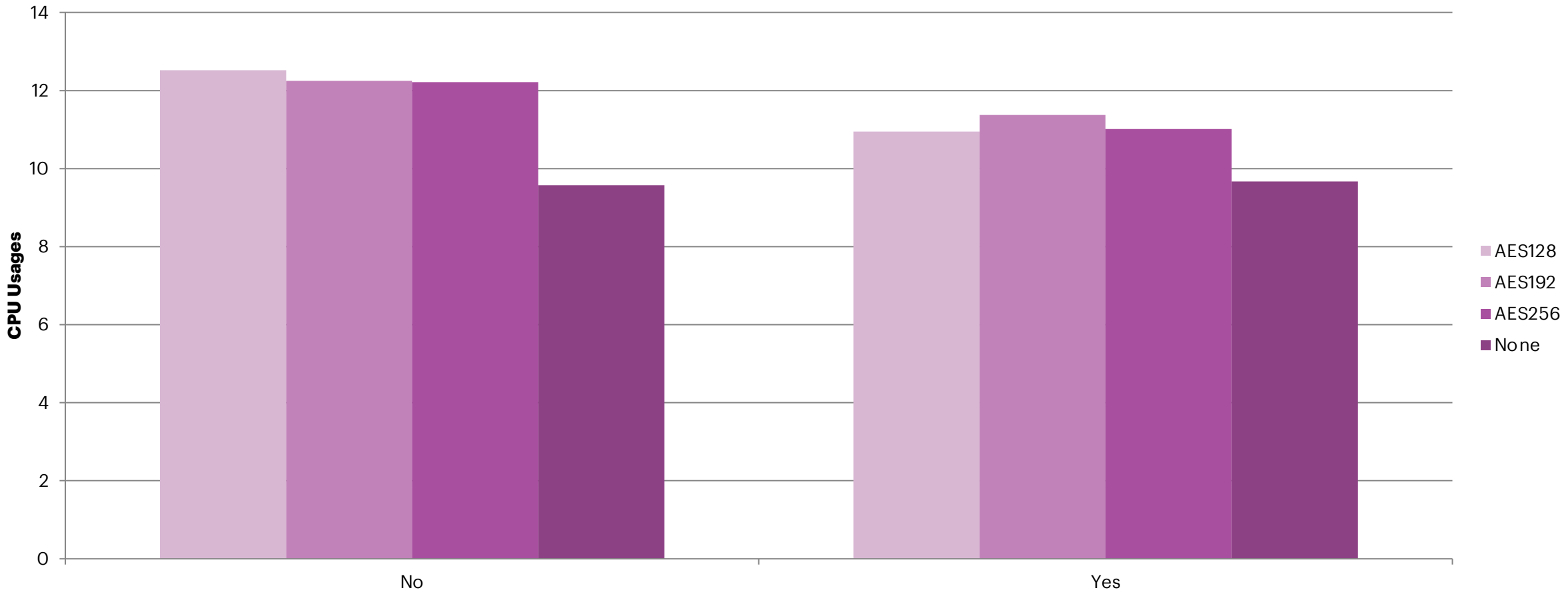
Performance Test Results

CPU time for TX details



Performance Test Results

CPU consumption in comparison for the AES algorithms



Performance Test Results

- In any case, TDE leads to a noticeably higher CPU utilization even with Hardware Cryptographic Acceleration
- Transactions per second are only different with a TDE tablespace above a certain workload
  Hardware Cryptographic Acceleration reduces CPU load by up to 30%.
- If applications generate more than 60% host CPU utilization at peak times, a CPU power upgrade may be necessary.
- It is recommended to do application **specific testing** before going live.

6

General Use Cases

Is AVDF a Product for your Database Environment?

Regular and Network

The basic to start

Regular Use Case

- Default database setup without any security measures e.g. no audit
- Serves as a reference for other setups

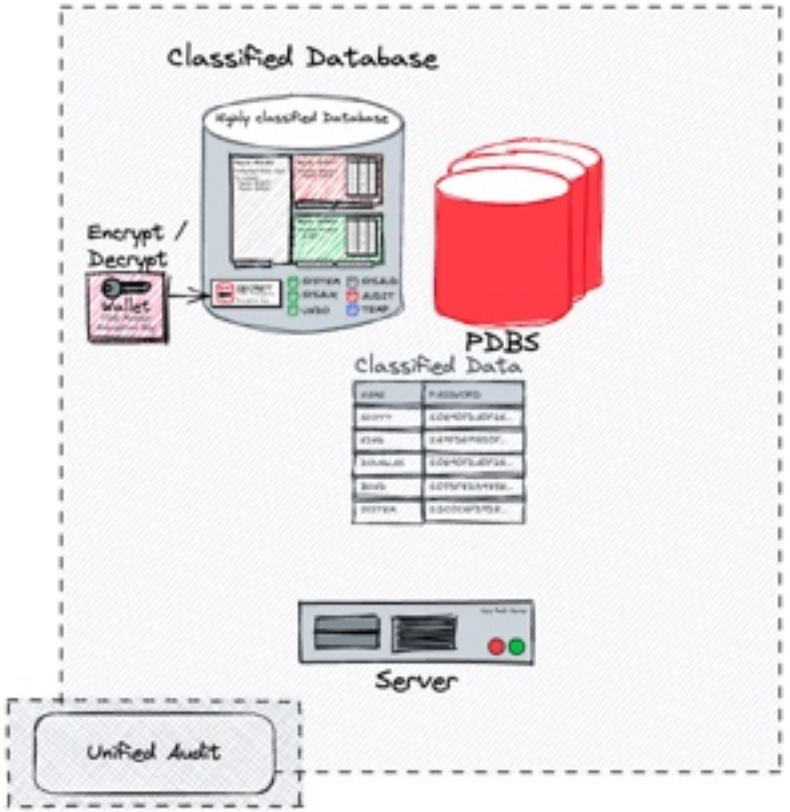
Network Use Case

- SQL Net native encryption
- SQL Net integrity checks with checksumm

Unified Audit

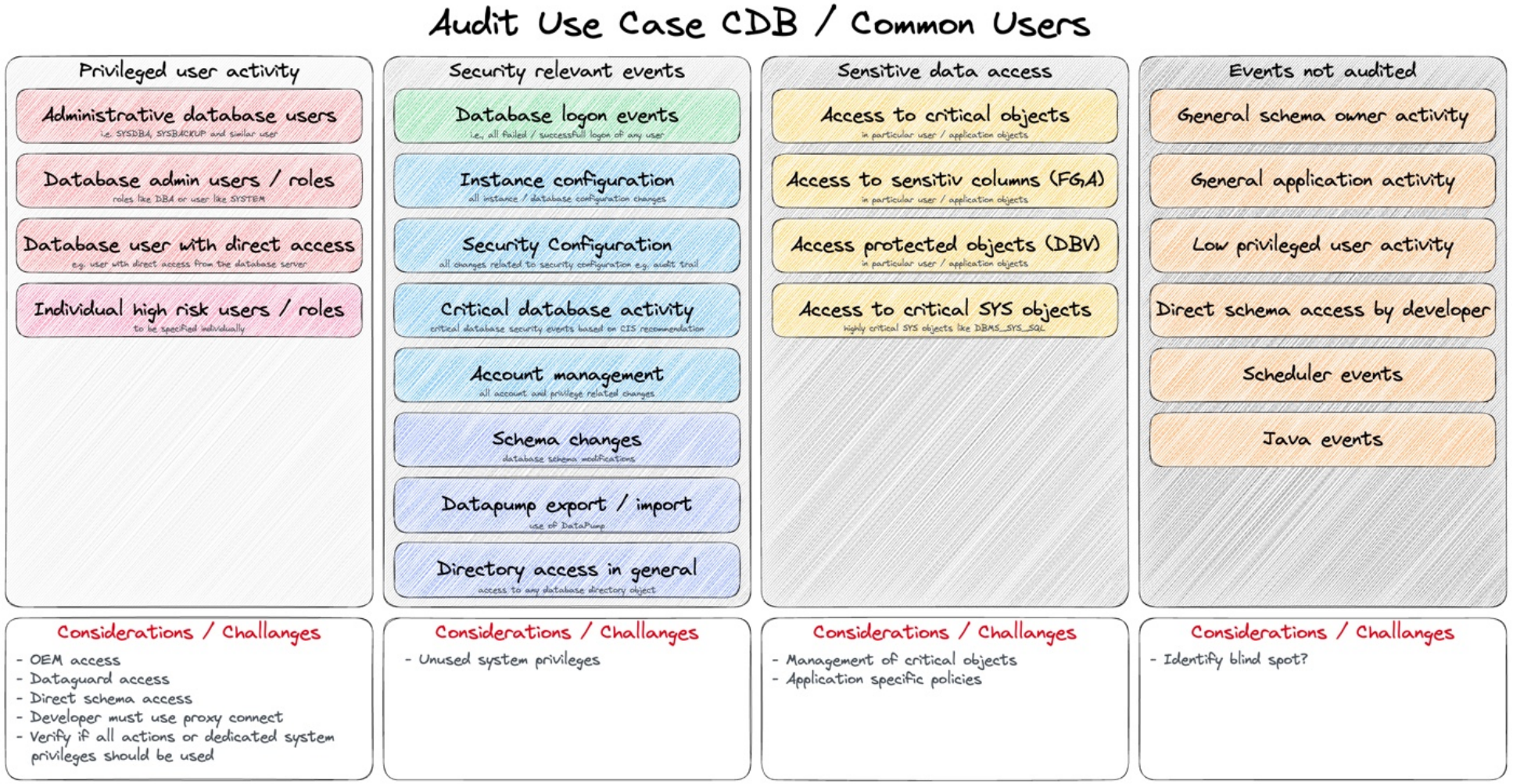
Various audit use cases and configurations

- Simple / default unified audit policies
- CIS recommended unified audit policies
- Admin (SYSDBA, DBA) full statement audit
- Full statement audit for schema owner
- Legacy audit without unified audit
- Unified audit with a per statement condition



Unified Audit

A couple of audit policies



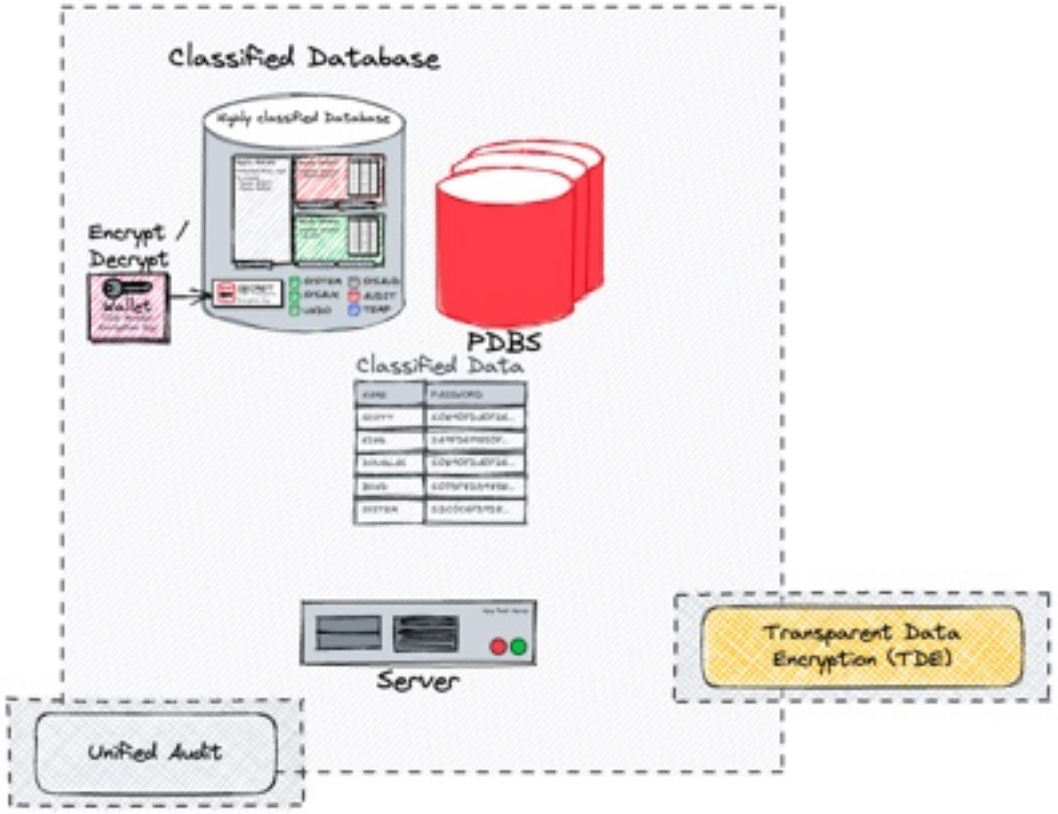
Oracle Transparent Data Encryption (TDE)

Tests and Tampering with Tablespace Encryption

- Encryption of tablespace used to store the Swingbench test Schema SOE
- Testing of different configurations and algorithms
  - AES 256 with Hardware Acceleration (default)
  - AES 256 without Hardware Acceleration
  - 3DES 168 legacy encryption algorithm
  - ARIA 256

Try to find things like

- Impact when using TDE
- Best encryption algorithm
- Idea for system setup / use case



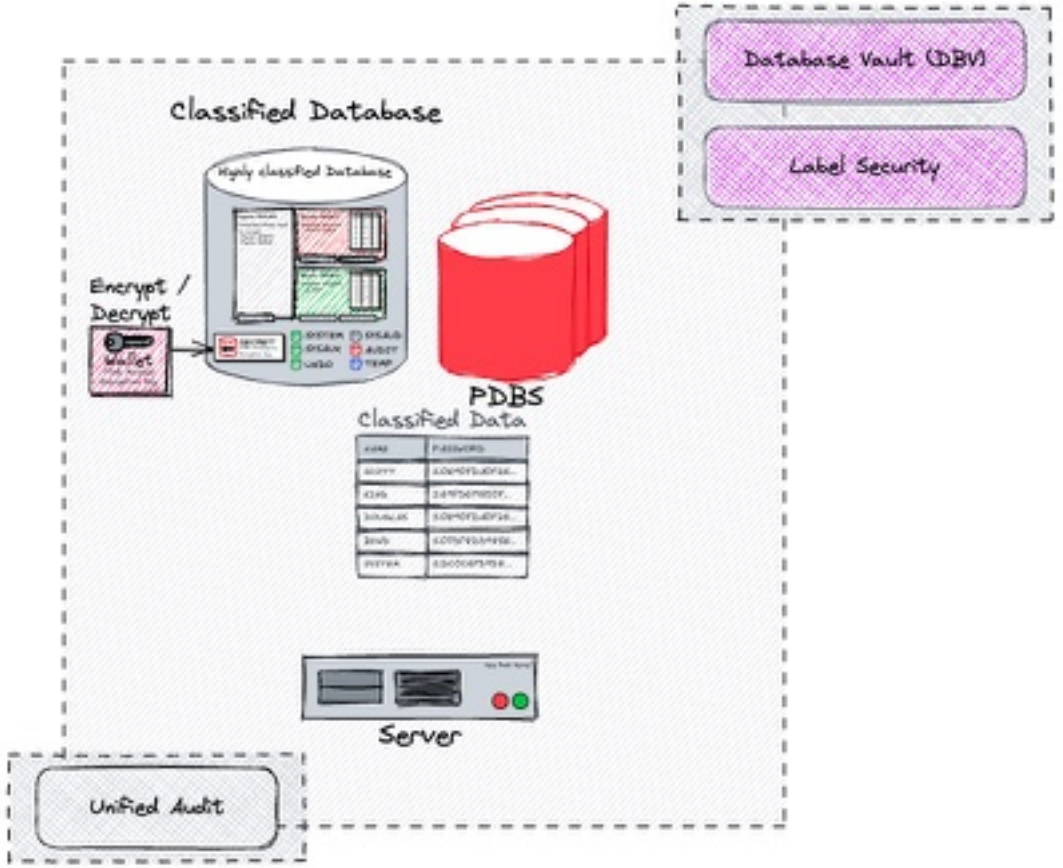
Oracle Database Vault

Protect SEO Schema using Database Vault

- Implement Database Vault in CDB$ROOT and PDB's
- Protect SOE schema with a DB vault Realm
- Simple initial setup

Try to find things like

- Impact when using DB Vault
- Particular issue with specific configurations



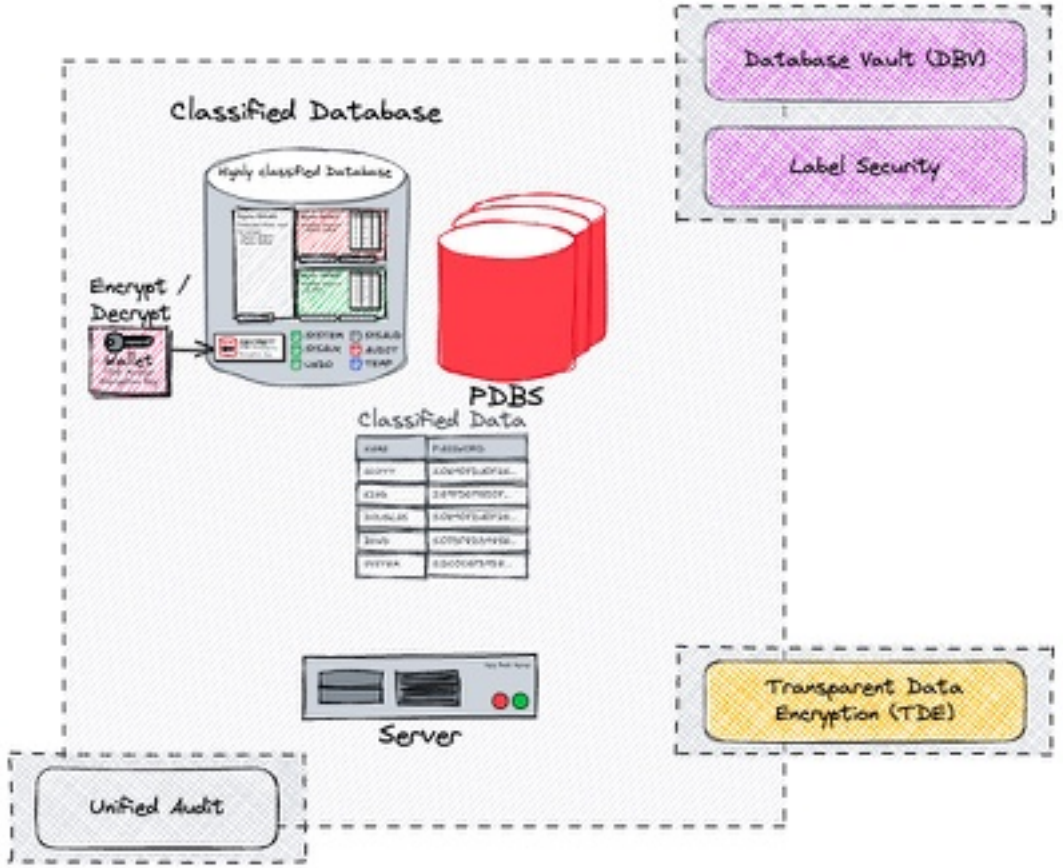
A secure Oracle Database

A first approach to put all together

- Configure SQLNetwork encryption and checksum
- Unified Audit with full CIS and Admin audit
- Transparent Data Encryption (TDE) for SOE data tablespace
- DB Vault Protection of SOE Schema

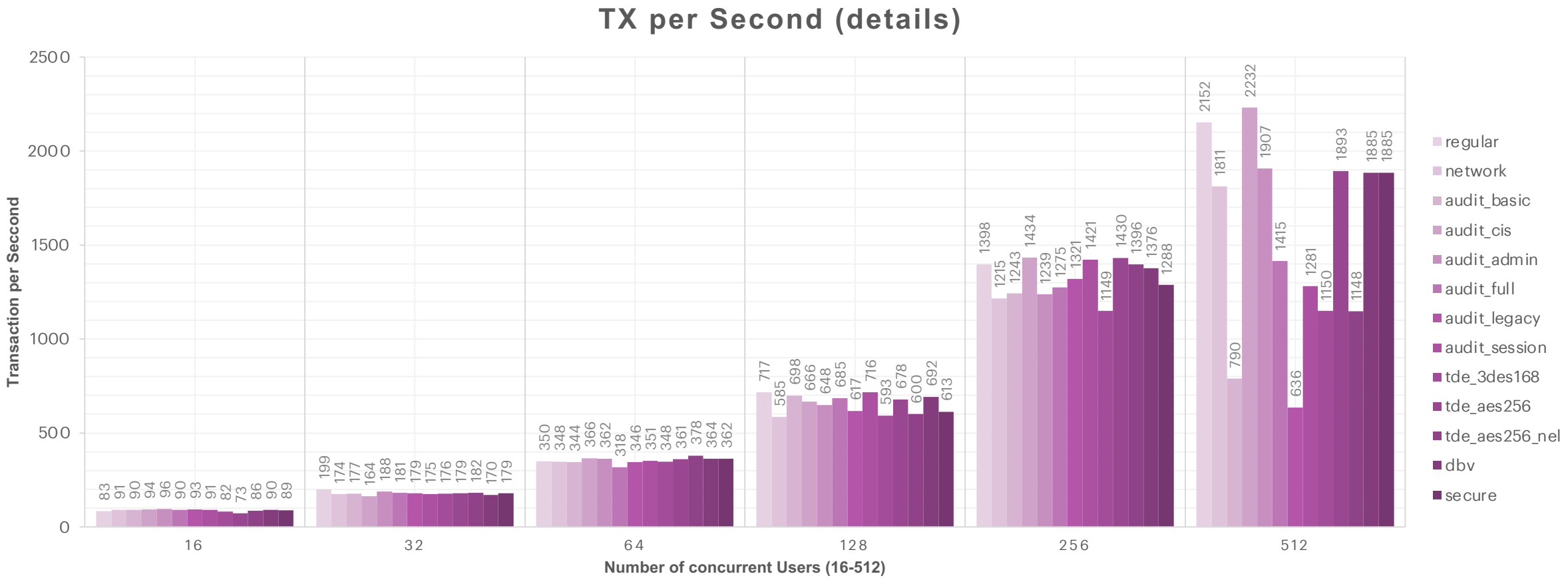
Try to find things like

- Impact when setup a secure configuration
- Behaviour when everything is combined
- Insides on potential configuration and good practice



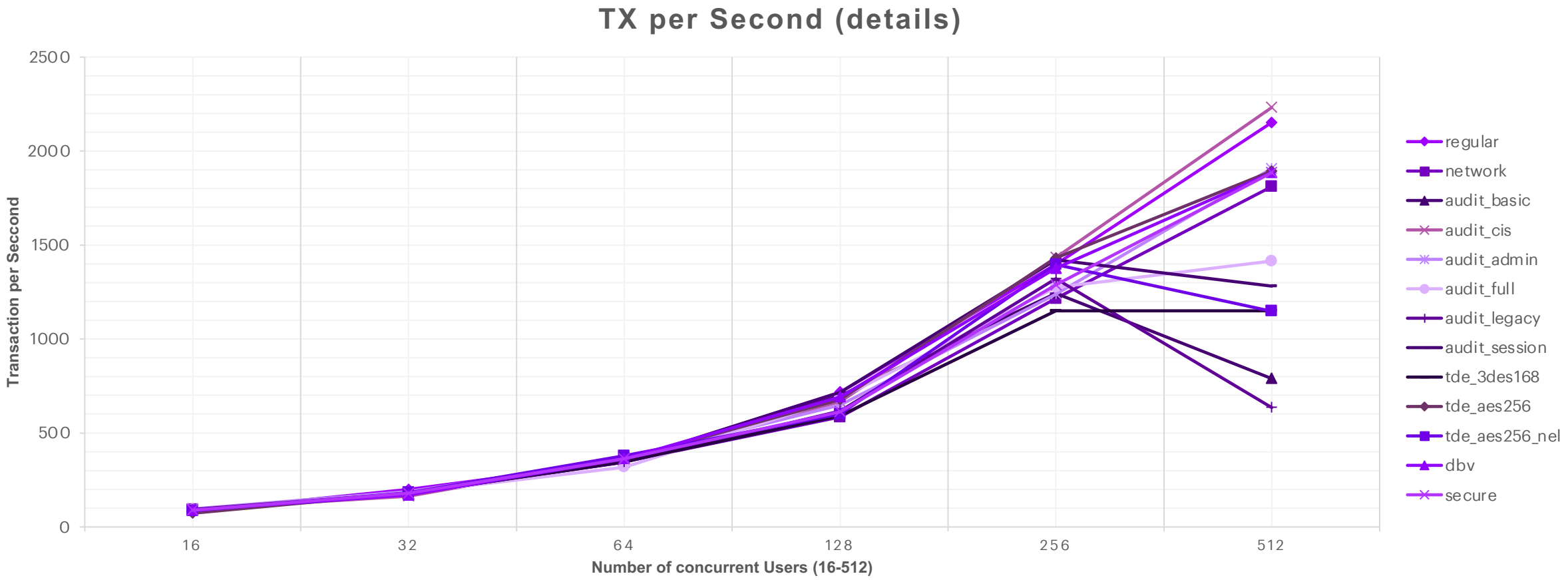
A sneek Preview

So now what's all about this security and performance?



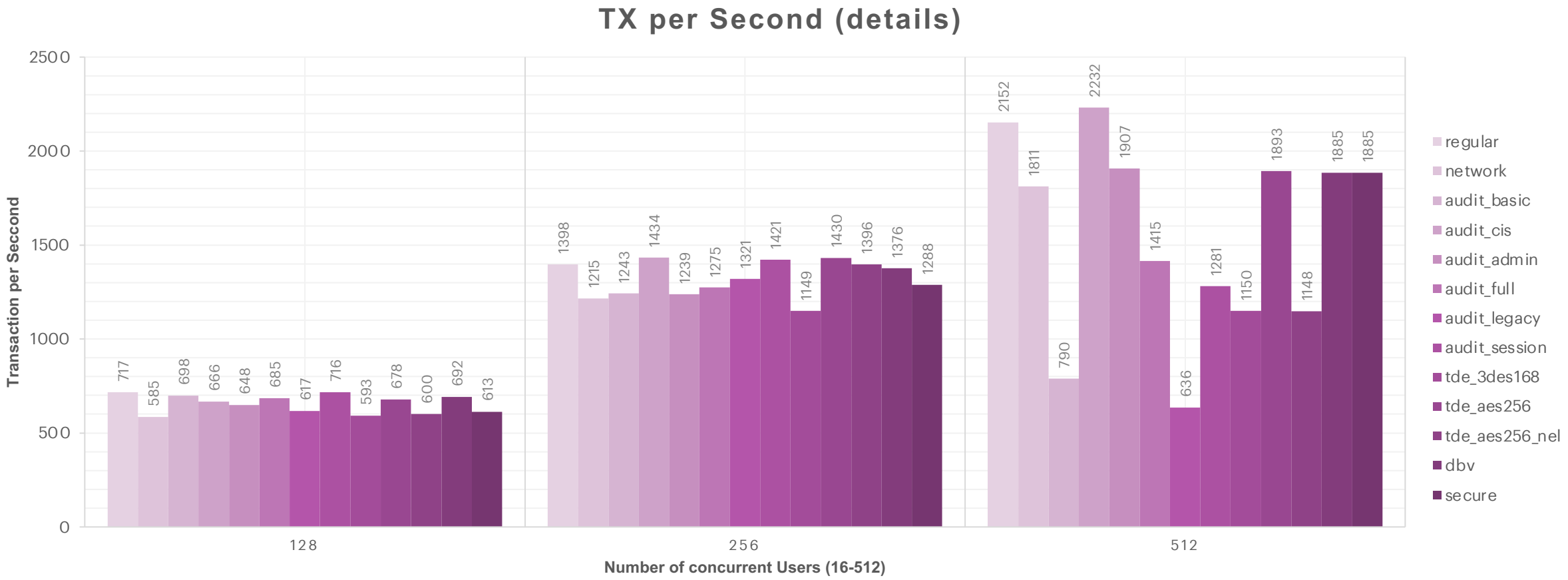
A sneek Preview

So now what's all about this security and performance?



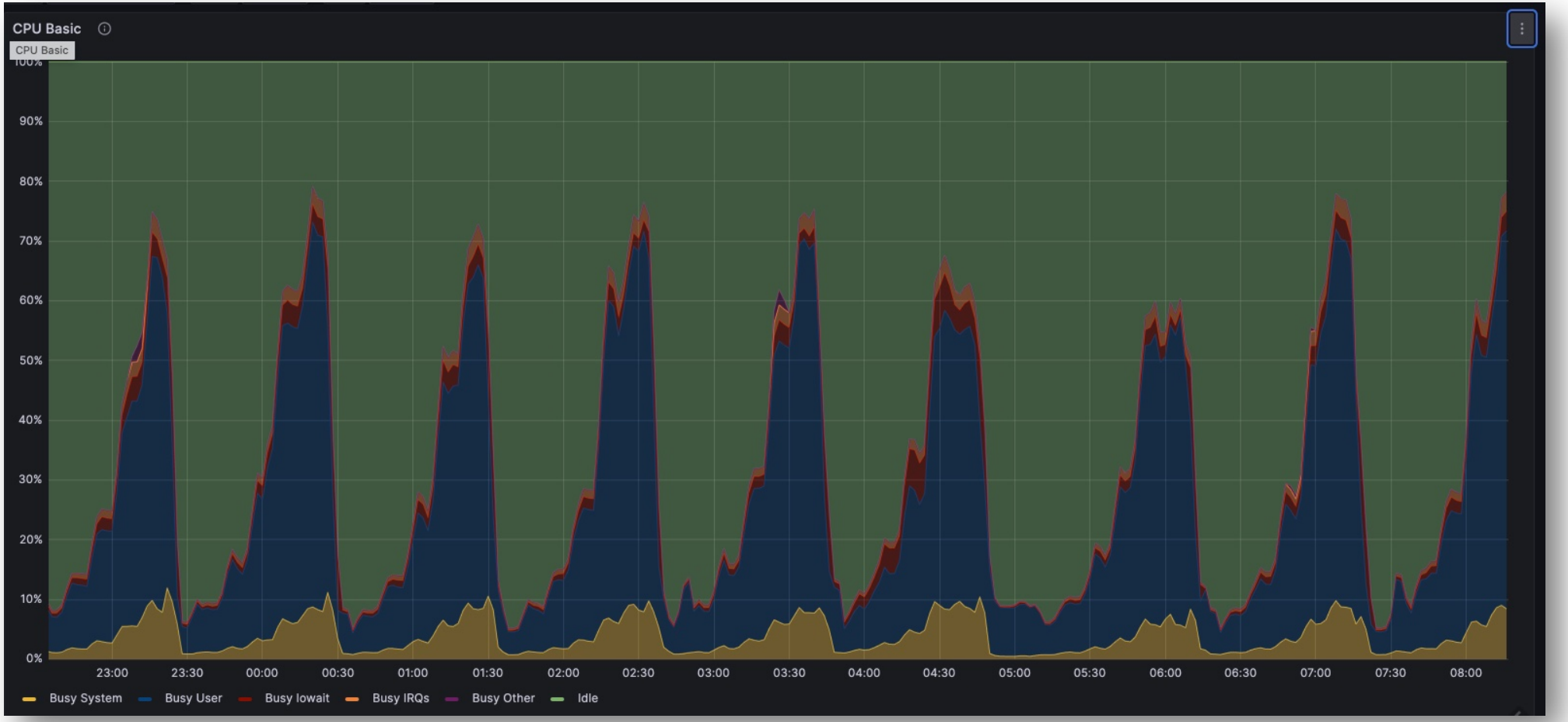
A sneek Preview

So now what's all about this security and performance?



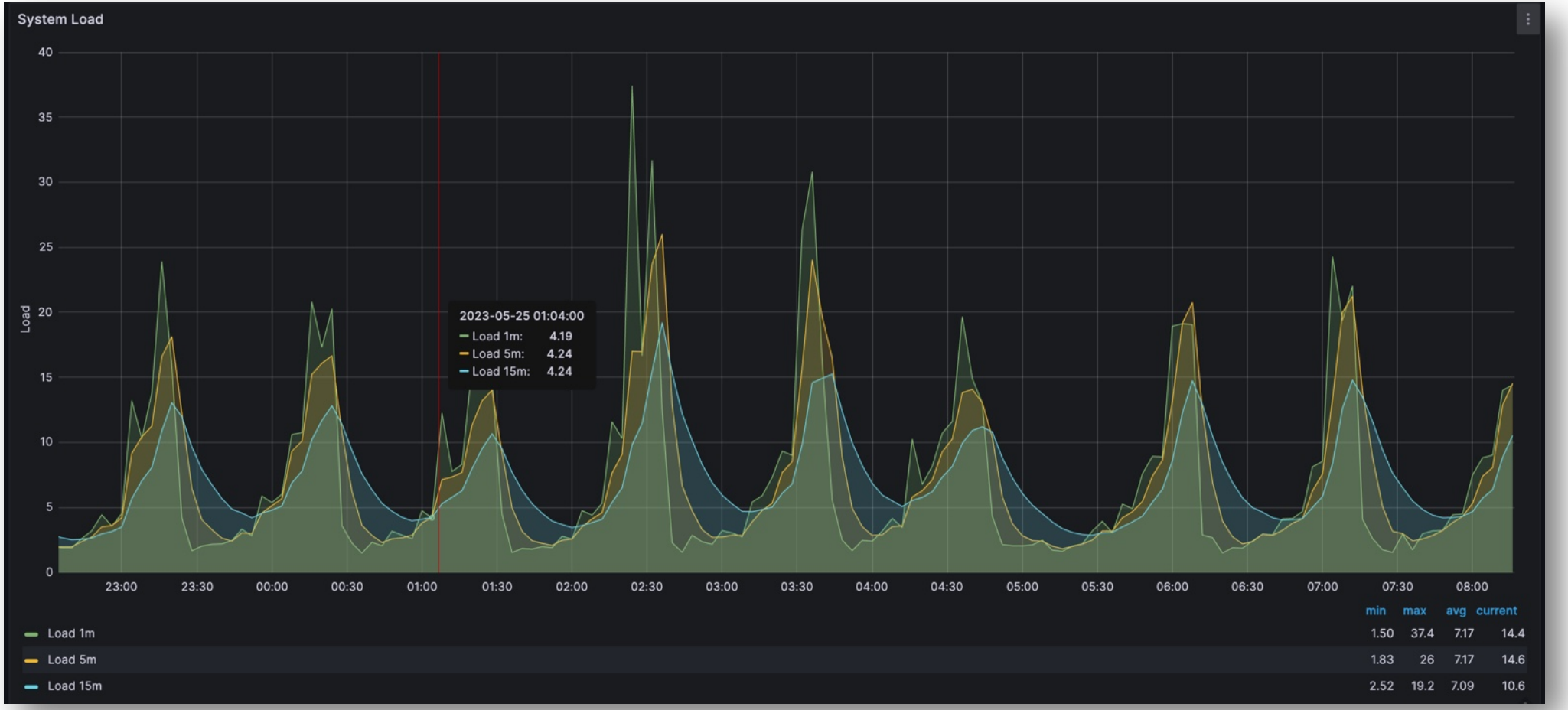
A sneek Preview

How does my CPU's look like?



A sneek Preview

And the system load?



7

What's Next?

Ideas and improvements for the future...

Ideas

Where is the journey going?

- Find the correct reference System (System Type, CPU, Memory, Storage)
  - Is a **physical system** required in any case?
- Finding a better and representative workload e.g. Workload **type**
  - Scale respective **size of workload schema** (25G or better 250GB)
  - **Tune workload** execution e.g. usual SwingBench tuning
  - **Special cases** must be analyzed in detail
- Fully **automate setup** of use cases as well execution
  - Make sure it is automated and repeatable including the **data evaluation**
  - Allow to run it on different Oracle version and patch levels
- Define additional database security use cases
  - Oracle Centrally Managed Users (CMU), Oracle Virtual Private Database (VPD), Oracle Fine Grained Auditing (FGA),...

Learnings...

Have I really learned anything?

- The idea is good. But it needs **more lead time**?
- **Shell** scripting is too convenient for me. And again I missed to check if there would have been **reasonable alternatives** e.g. Ansible,...
- OCI Bare Metal System is **relatively quick** to deploy, but it **does cost a bit**
- The whole thing would be a good **interdisciplinary** topic... let's team up!
  - Where were incorrect assumptions made?
  - What side effects were overlooked?
- Will my technical presentations be ready 4 weeks in advance? Nah, **I don't think so** 😎
- My wife doesn't like it when I **crash** a Lab system at home and swear.

8

Conclusion

Now, what about the performance of security features?

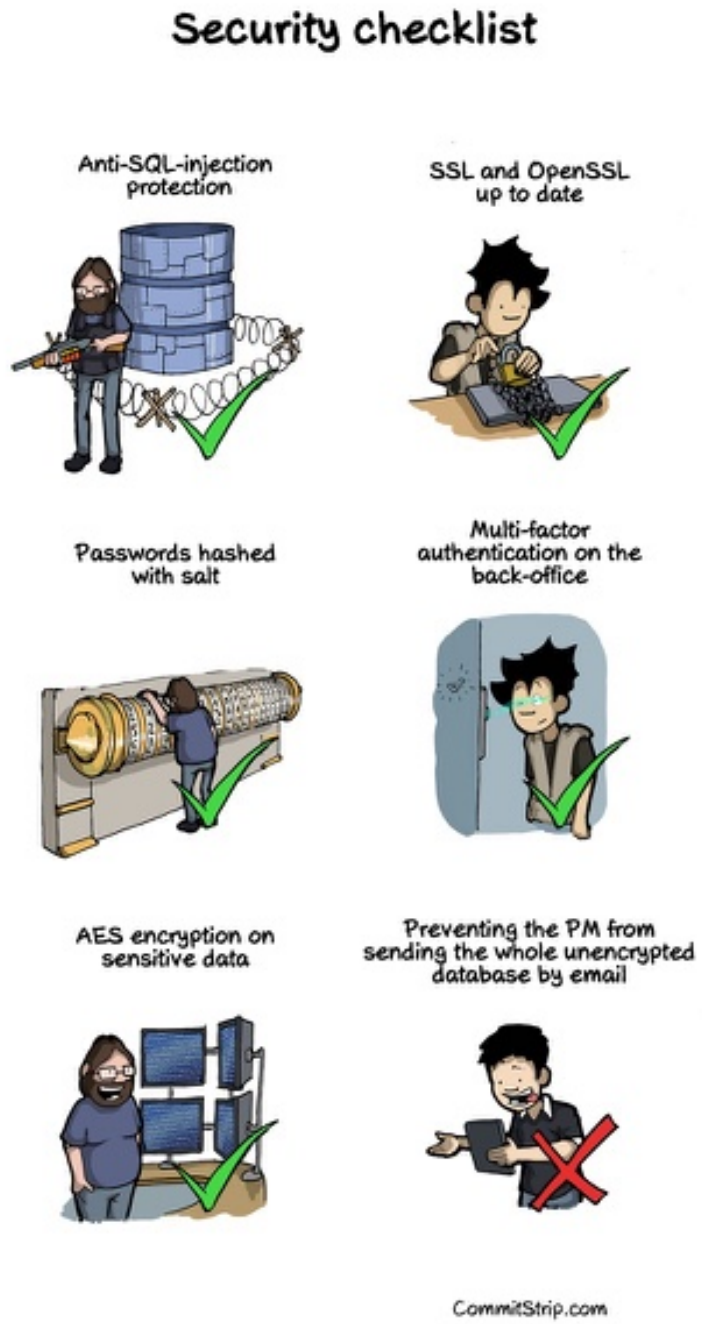
Conclusion

Is there a performance formular for security features / options?

- There is **no clear** answer
- The impact **largely depends** on the environment, e.g. workload, base load, peak load, CPUs, memory, IO, etc.

Important takeaways:

- **Do your homework**
  - How so you need which Features?
  - Only as much as necessary, not as possible!
  - Not everything is reasonable/possible
- A heavily loaded system does not like any change!
- Proper **requirements analysis**
  - Security feature not selected according to performance aspects
- Consider a real **regression test** in your environment



The biggest challenge is still to define the requirements and the appropriate security concept of the databases...

References

Not enough yet? Below a few links to explore the topic in more depth.

- Oracle® Database Advanced Security Guide 21c
  - Chapter 10.3 Performance and Storage Overhead of Transparent Data Encryption
  - Chapter 13.2 Performance Questions About Transparent Data Encryption
- Swingbench by Dominic Giles
- SecBench GitHub Repository oehrlis/secbench (still work in progress)
- Blog post www.oradba.ch I'll definitely stay on track and will write one or two other post about it.
- Oracle Database Unified Audit Best Practice Guidelines
- And all kind of Oracle Documentation and whitepapers.

Thank You