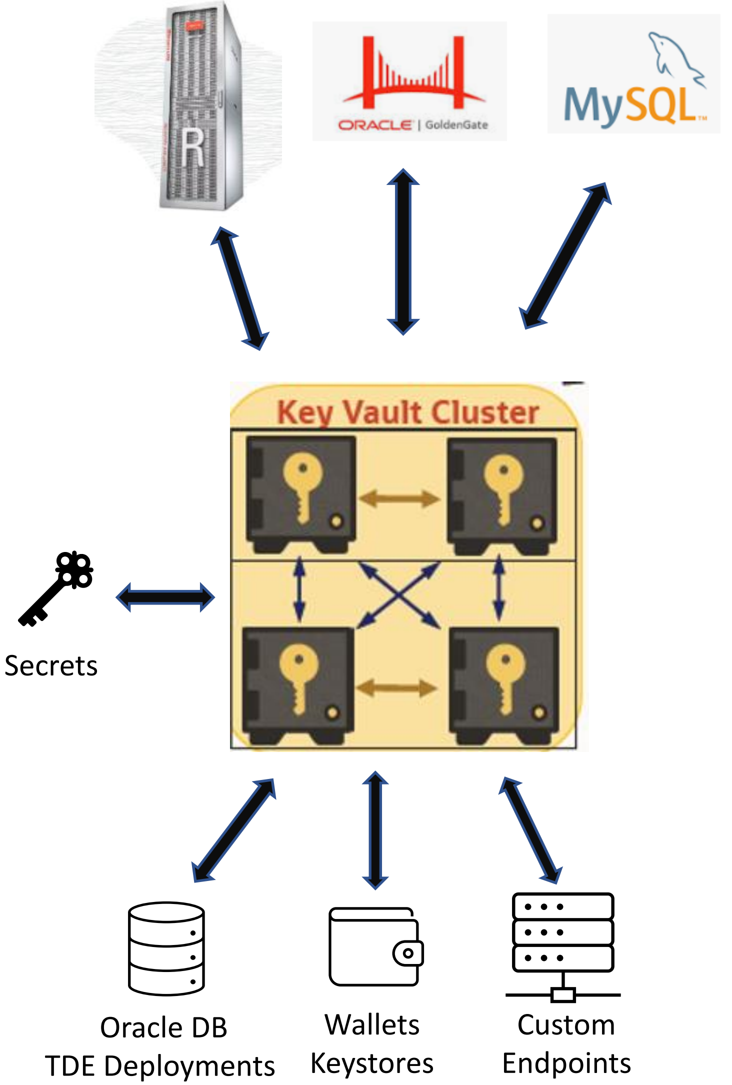
Oracle Key Vault Introduction (use case with Exa@CC Gen2)



Key Vault Cluster

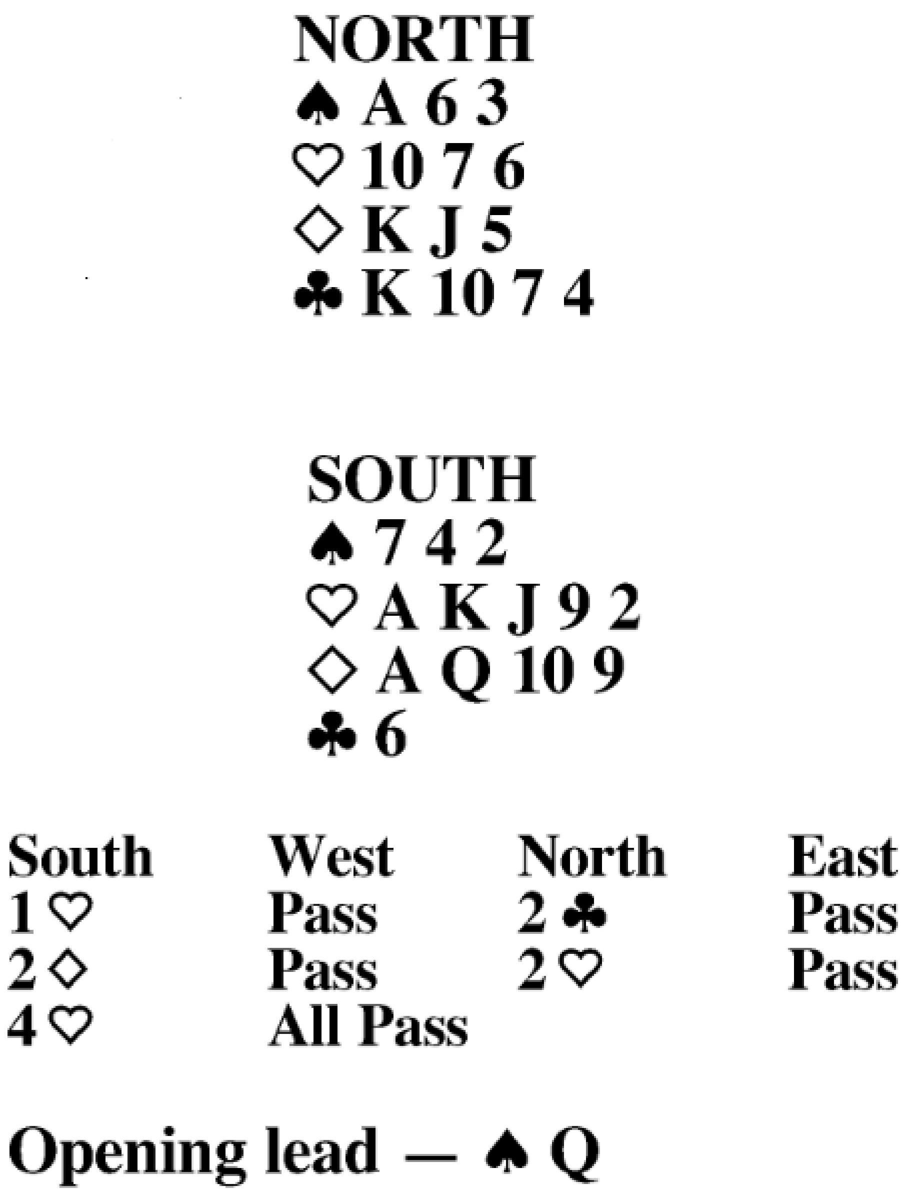
Secrets

Oracle DB TDE Deployments

Wallets Keystores

Custom Endpoints

accenture



NORTH
♠ A 6 3
♡ 10 7 6
◇ K J 5
♣ K 10 7 4

SOUTH
♠ 7 4 2
♡ A K J 9 2
◇ A Q 10 9
♣ 6

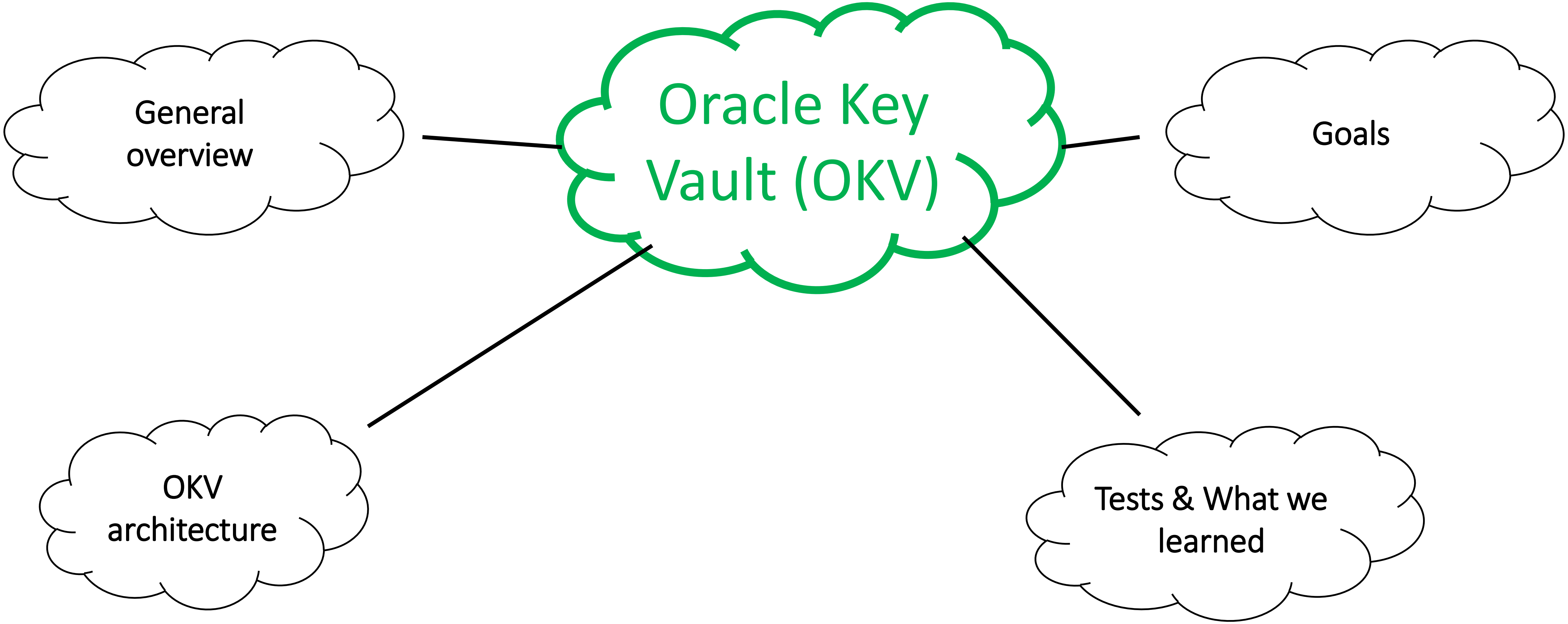
South	West	North	East
1♡	Pass	2♣	Pass
2◇	Pass	2♡	Pass
4♡	All Pass		

Opening lead — ♠ Q

Dealing with technology is like contract bridge. A suboptimal plan is better than none. You nearly always have not enough time to find optimal one. Find good enough!

***Krzysztof Martens** – Bridge Grand Master, ca. 2005*

Agenda



Oracle Key Vault (OKV)

General overview

Goals

OKV architecture

Tests & What we learned

Oracle Key Vault & Goal. What we had to todo?

Requirements – business view

We have 3 months for finish everything.

Oracle Key Vault – maximum security please.

No. We don’t have budget for order enything more.

Yes. We already have everything designed and prepared. Previous vendor prepared everything.

We are using Google Cloud for everything in this project except databases – Exa@CC. Oracle Key Vault should be deployed there.

Integration with existing systems – authorization, certification managament

Yes. We already have everything designed and prepared.

Oracle Key Vault maintenance should have no impact on databases’ availability.

Create procedures for operations

Architectural decisions & Technical Debt

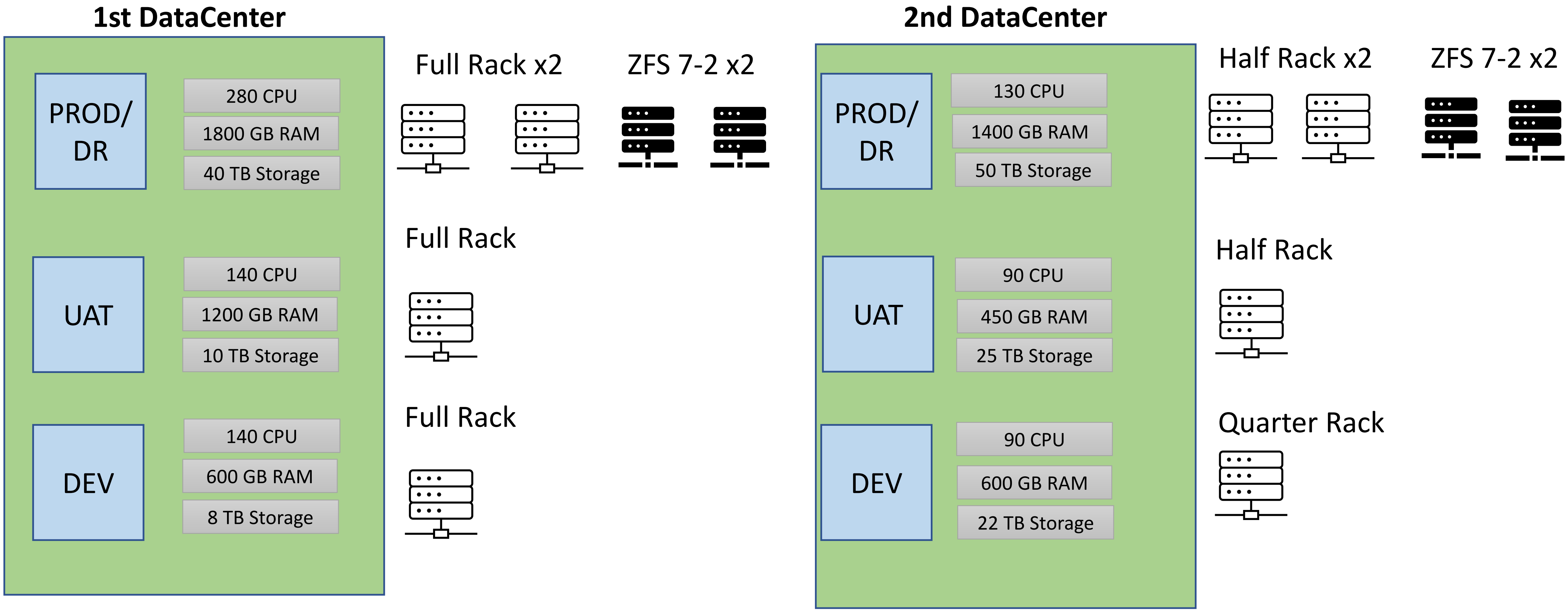
TECHNICAL DEBT
I DON'T UNDERSTAND WHY IT TAKES SO LONG TO ADD A NEW WINDOW.
@VINCENTDNL

source

Not all projects start from scratch when you start working on them ☹

Goal

- Migrate **65 databases** (both TDE encrypted and noth encrypted) to Exa@CC gen2 and HPE blades with **central keystore** in Oracle Key Vault. **80TB** of data in total
- We are using Multiple VMs per Exadata feature
- OKV deployed on HPE Blades (bare-metal) using 4 nodes for whole environment
- Support for both Exa@CC and non-Exa@CC workloads (non-Exa used due to client's requirement)



1st DataCenter

PROD/ DR

280 CPU

1800 GB RAM

40 TB Storage

UAT

140 CPU

1200 GB RAM

10 TB Storage

DEV

140 CPU

600 GB RAM

8 TB Storage

Full Rack x2

ZFS 7-2 x2

Full Rack

Full Rack

2nd DataCenter

PROD/ DR

130 CPU

1400 GB RAM

50 TB Storage

UAT

90 CPU

450 GB RAM

25 TB Storage

DEV

90 CPU

600 GB RAM

22 TB Storage

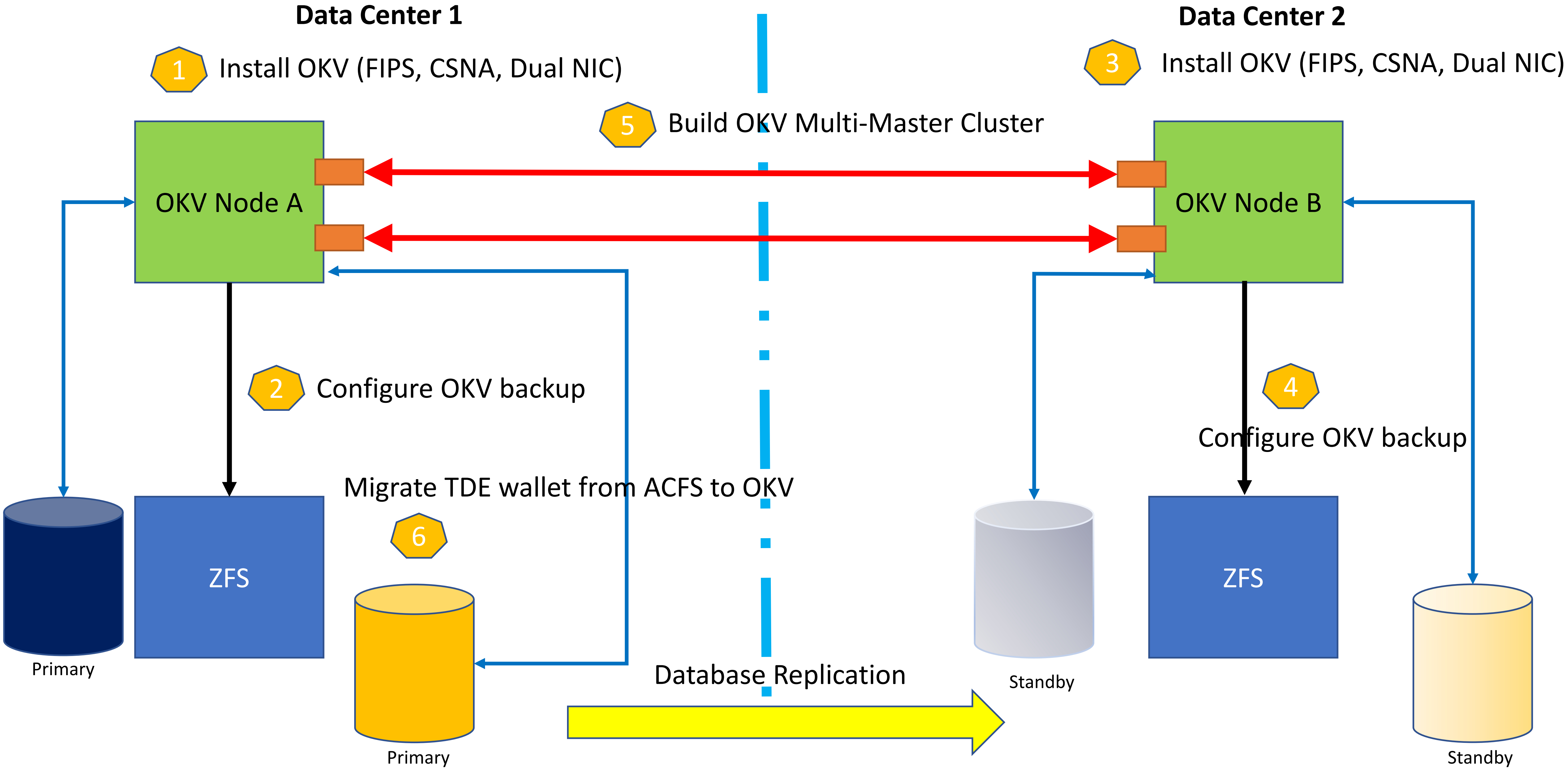
Half Rack x2

ZFS 7-2 x2

Half Rack

Quarter Rack

OKV Deployment Plan (Exa@CC Gen2 and OKV 21.5, ZFS 7.2)



OCI-based database deployment and OKV

- ❑ **Out-of-the Box** OKV integration with Exa@CC Gen2 **only possible with Autonomous Databases** on Exa@CC Gen2 (ADB-ExaC@C Gen2). For non-Autonomus Database integration requires additional work.

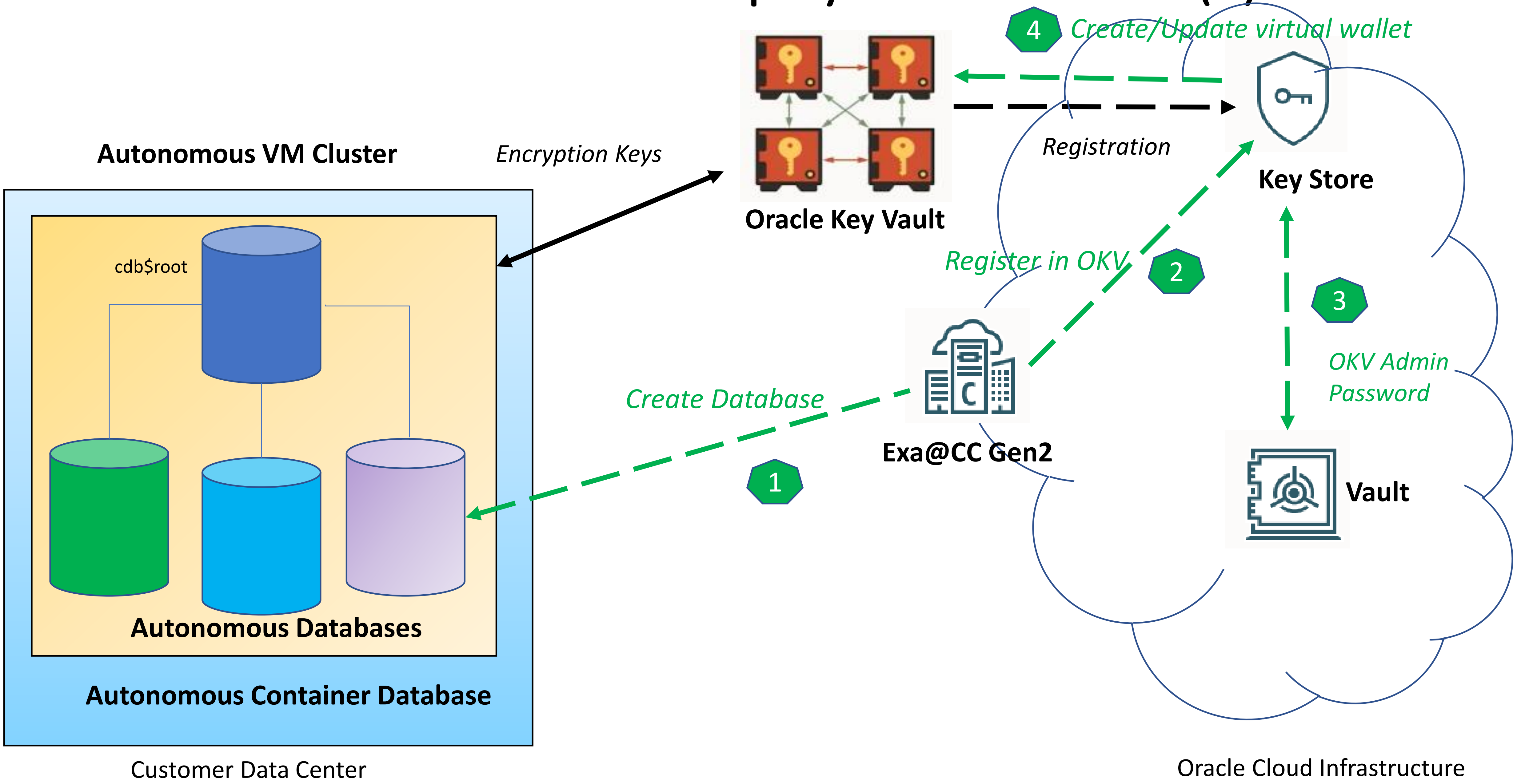
- ❑ Main Use Case for integration is **automatic registration**. It applies this key management resource to all new ExaDB-D databases during their provisioning time.

- ❑ Already deployed databases **will not be** automatically migrated from file-based wallet. You have to migrate them.

- ❑ Standard Exa@CC Gen2 integration with OKV is not in roadmap (state from **March 2023**)

- ❑ OKV endpoint **self-assessment** (a.k.a auto-assessment) cannot be used
  - ❖ Not practical for Exa@CC Gen2 databases where they are RAC-based databases. Virtual wallet is shared for all instances in RAC database (primary + standby). Self-assessment creates separated wallet for each instance ☹
  - ❖ In deprecated state since release 21.5

OCI-based database deployment and OKV (2)



Exa@CC Gen2 and OKV - limitations

- Data Guard Associations Across Regions (Data Guard / Active Data Guard)
  – only possible for databases with local TDE wallets, not possible with OKV

  Create Data Guard configuration and later migrate to OKV

- Exa@CC Gen2 Non-Autonomous – no automatic encryption keys provisioning in OKV for new databases

  All new databases using standard TDE wallet placed on ACFS
  You have to migrate wallet to OKV after database provisioning

- No keystore integration for Exa@CC Gen Non-Autonomous db in OCI Console

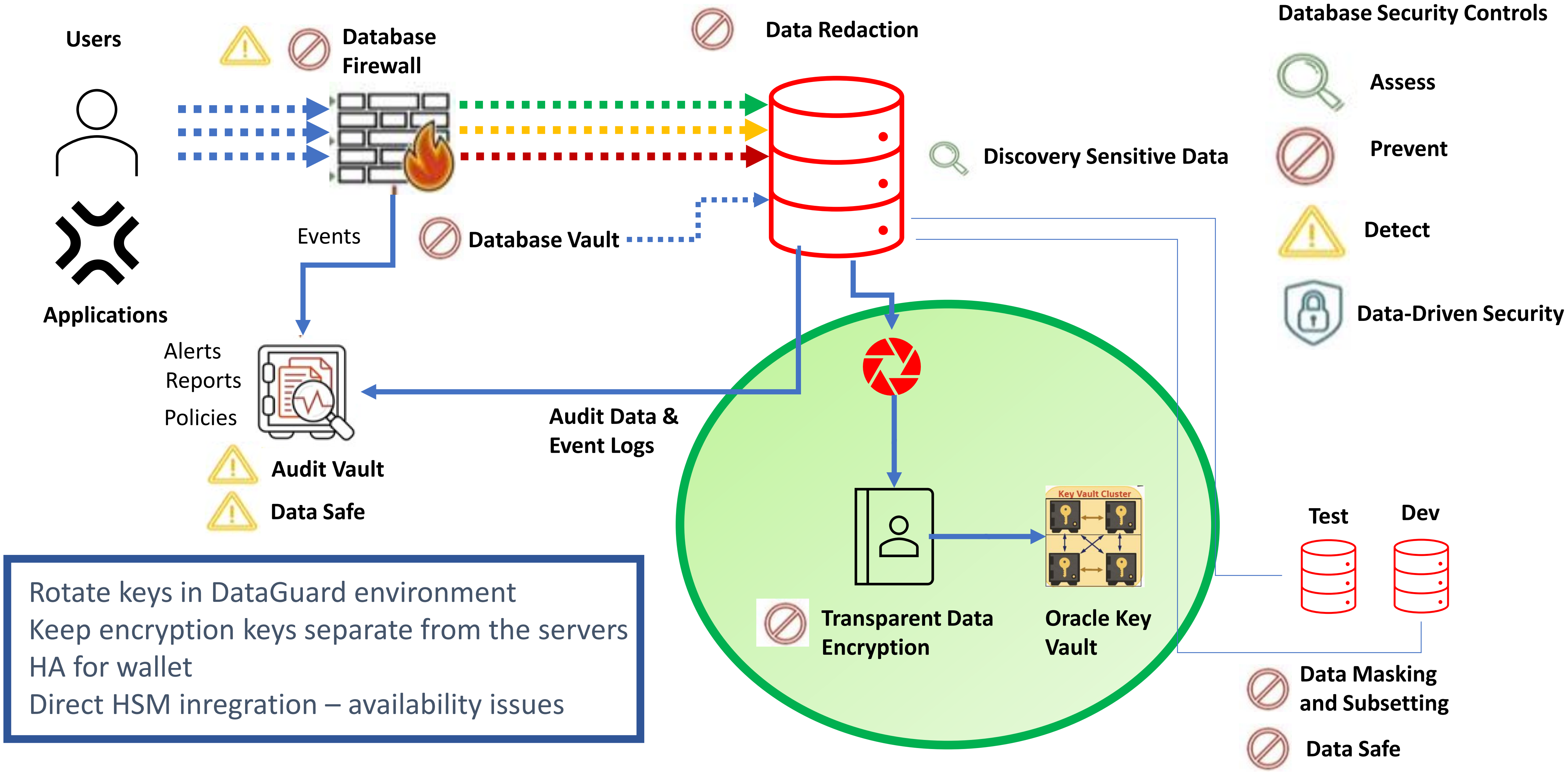
  It was true when we performed work, but ……. **5 months** after finishing deployment and migration……..

26th July 2023 - **Oracle Key Vault (OKV) Integration with ExaDB-C@C to Managed TDE Keys**

It’s not possible to attach existing keystores to OCI console ☹ …. but we are working with Oracle to allow this option ☺ Maybe automatic registration in OKV for new database will be possible ….

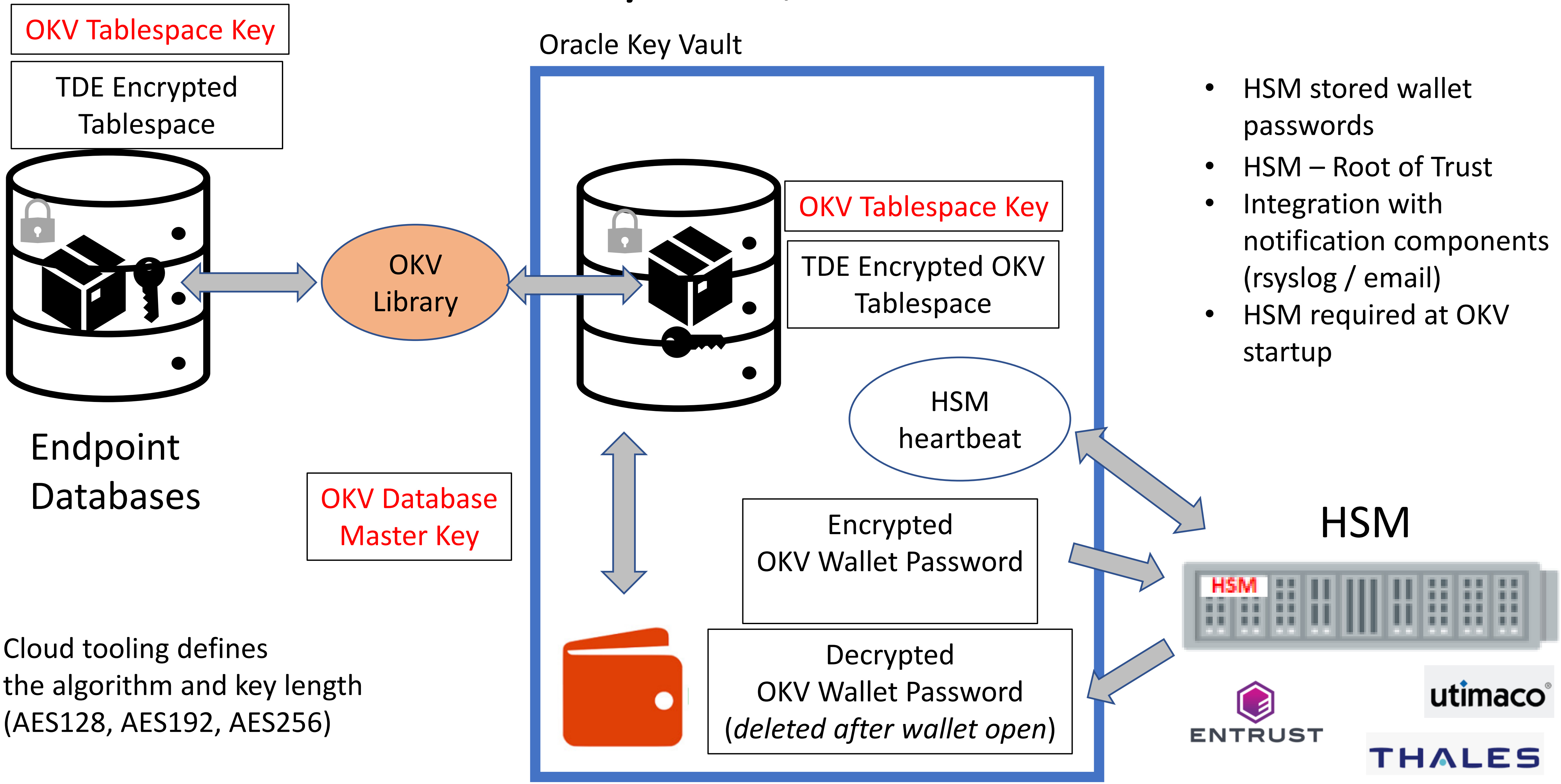
Oracle Key Vault - General Overview

OKV place in Oracle Maximum Security Architecture



Rotate keys in DataGuard environment
Keep encryption keys separate from the servers
HA for wallet
Direct HSM inregration – availability issues

Oracle Key Vault, TDE and HSM



OKV Tablespace Key

TDE Encrypted Tablespace

Endpoint Databases

OKV Library

OKV Database Master Key

Oracle Key Vault

OKV Tablespace Key

TDE Encrypted OKV Tablespace

HSM heartbeat

Encrypted OKV Wallet Password

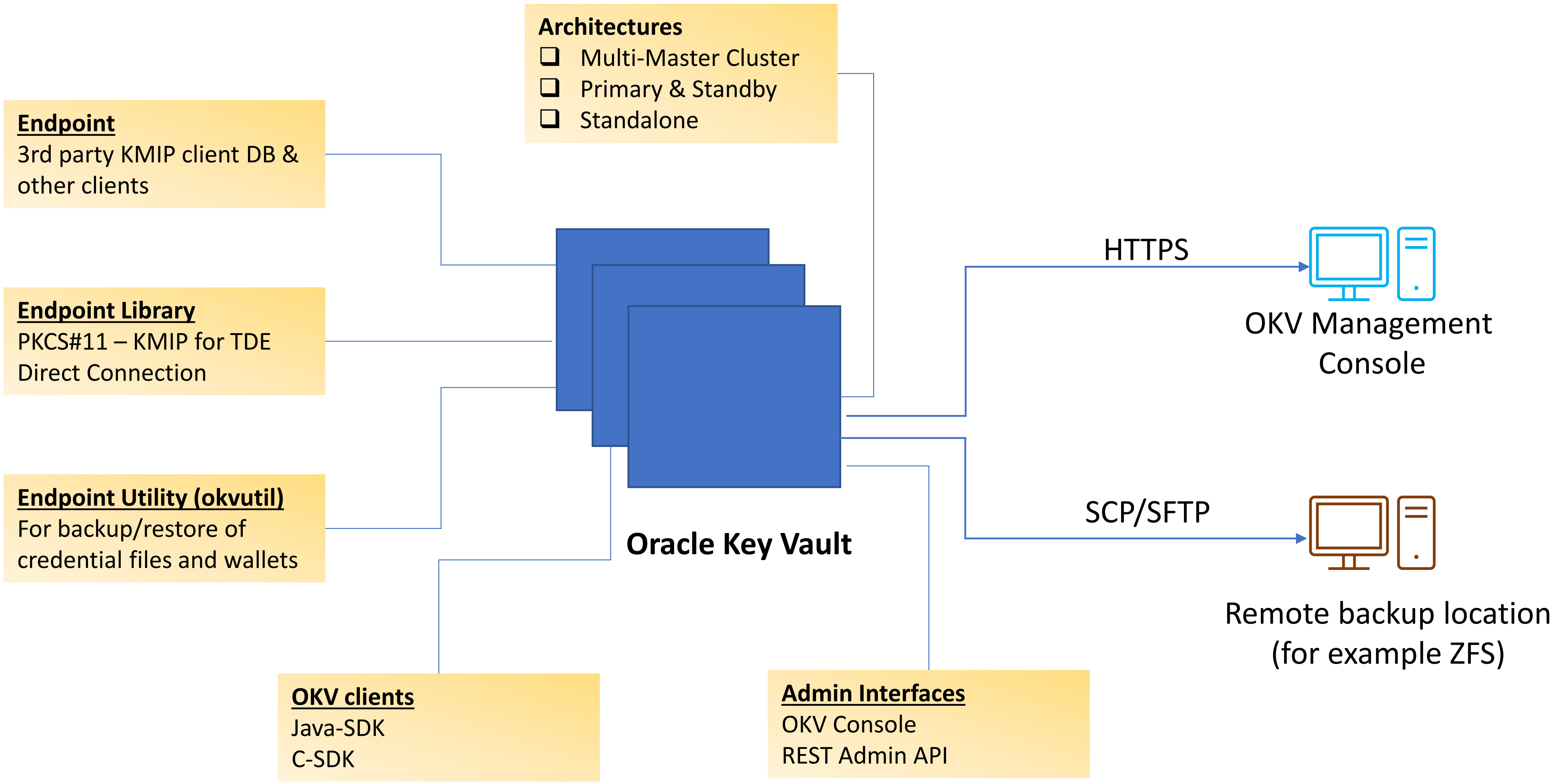
Decrypted OKV Wallet Password *(deleted after wallet open)*

HSM

- HSM stored wallet passwords
- HSM – Root of Trust
- Integration with notification components (rsyslog / email)
- HSM required at OKV startup

Cloud tooling defines
the algorithm and key length
(AES128, AES192, AES256)

OKV – Key Facts



Architectures

□ Multi-Master Cluster

□ Primary & Standby

□ Standalone

Endpoint

3rd party KMIP client DB & other clients

Endpoint Library

PKCS#11 – KMIP for TDE

Direct Connection

Endpoint Utility (okvutil)

For backup/restore of credential files and wallets

Oracle Key Vault

HTTPS

OKV Management Console

SCP/SFTP

Remote backup location (for example ZFS)

OKV clients

Java-SDK

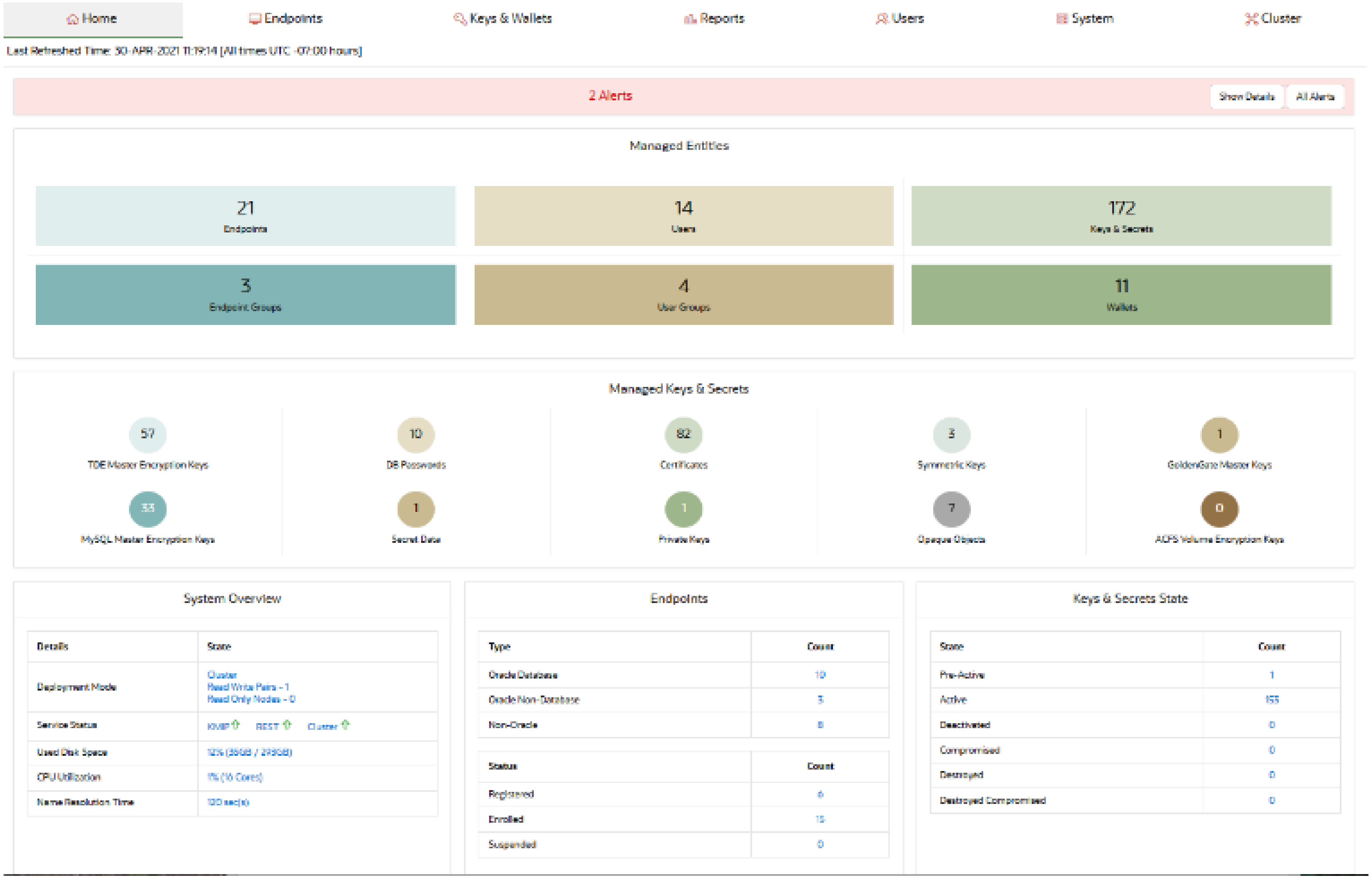
C-SDK

Admin Interfaces

OKV Console

REST Admin API

OKV Console



Last Refreshed Time: 30-APR-2021 11:19:14 [All times UTC -07:00 hours]

2 Alerts

Managed Entities

21 Endpoints

14 Users

172 Keys & Secrets

3 Endpoint Groups

4 User Groups

11 Wallets

Managed Keys & Secrets

57 TDE Master Encryption Keys

33 MySQL Master Encryption Keys

10 DB Passwords

1 Secret Data

82 Certificates

1 Private Keys

3 Symmetric Keys

7 Opaque Objects

1 GoldenGate Master Keys

0 ACFS Volume Encryption Keys

System Overview

Details	State
Deployment Mode	Cluster Read Write Pairs - 1 Read Only Nodes - 0
Service Status	KMIP ⇧ REST ⇧ Cluster ⇧
Used Disk Space	12% (35GB / 293GB)
CPU Utilization	1% (16 Cores)
Name Resolution Time	120 sec(s)

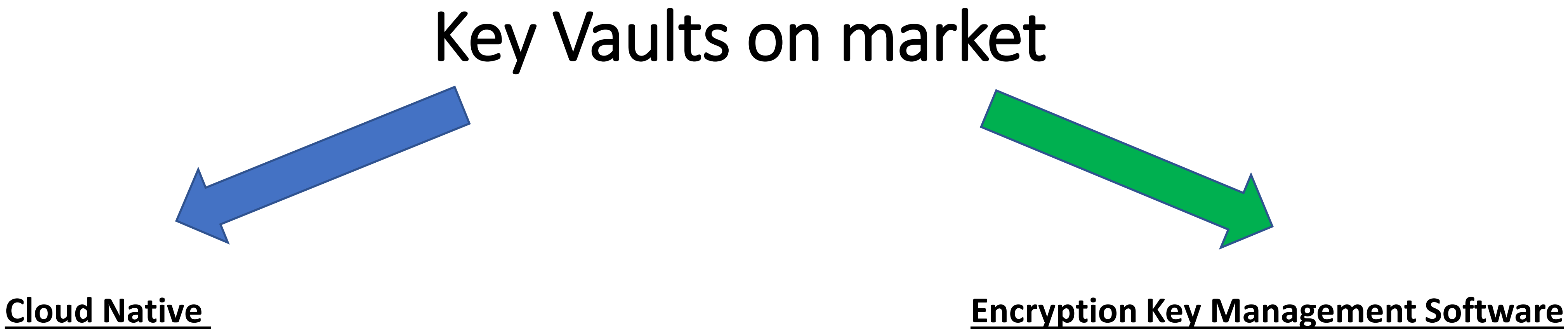
Endpoints

Type	Count
Oracle Database	10
Oracle Non-Database	3
Non-Oracle	8

Status	Count
Registered	6
Enrolled	15
Suspended	0

Keys & Secrets State

State	Count
Pre-Active	1
Active	155
Deactivated	0
Compromised	0
Destroyed	0
Destroyed Compromised	0



Key Vaults on market

Cloud Native

- AWS RDS – AWS KMS
- Azure TDE and Always Encrypted
- GCP Encrypted Service
- OCI Vault
- Alibaba Cloud and TDE
- IBM Cloud – Key Protect

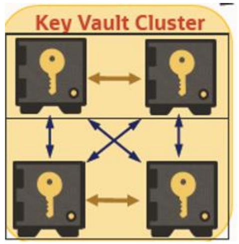
Encryption Key Management Software

- HashiCorp Vault
- Thales Vormetric Data Security Manager
- Oracle Key Vault

Oracle Key Vault vs OCI Vault

Oracle Key Vault

- Support **both** on-premises/hybrid and OCI workloads
- Support Oracle Exa@CC and Oracle Autonomous
- Golden Gate & ACFS encryption tasks integration possiblity
- Customer-Managed Encryption
- Software & HSM protected keys



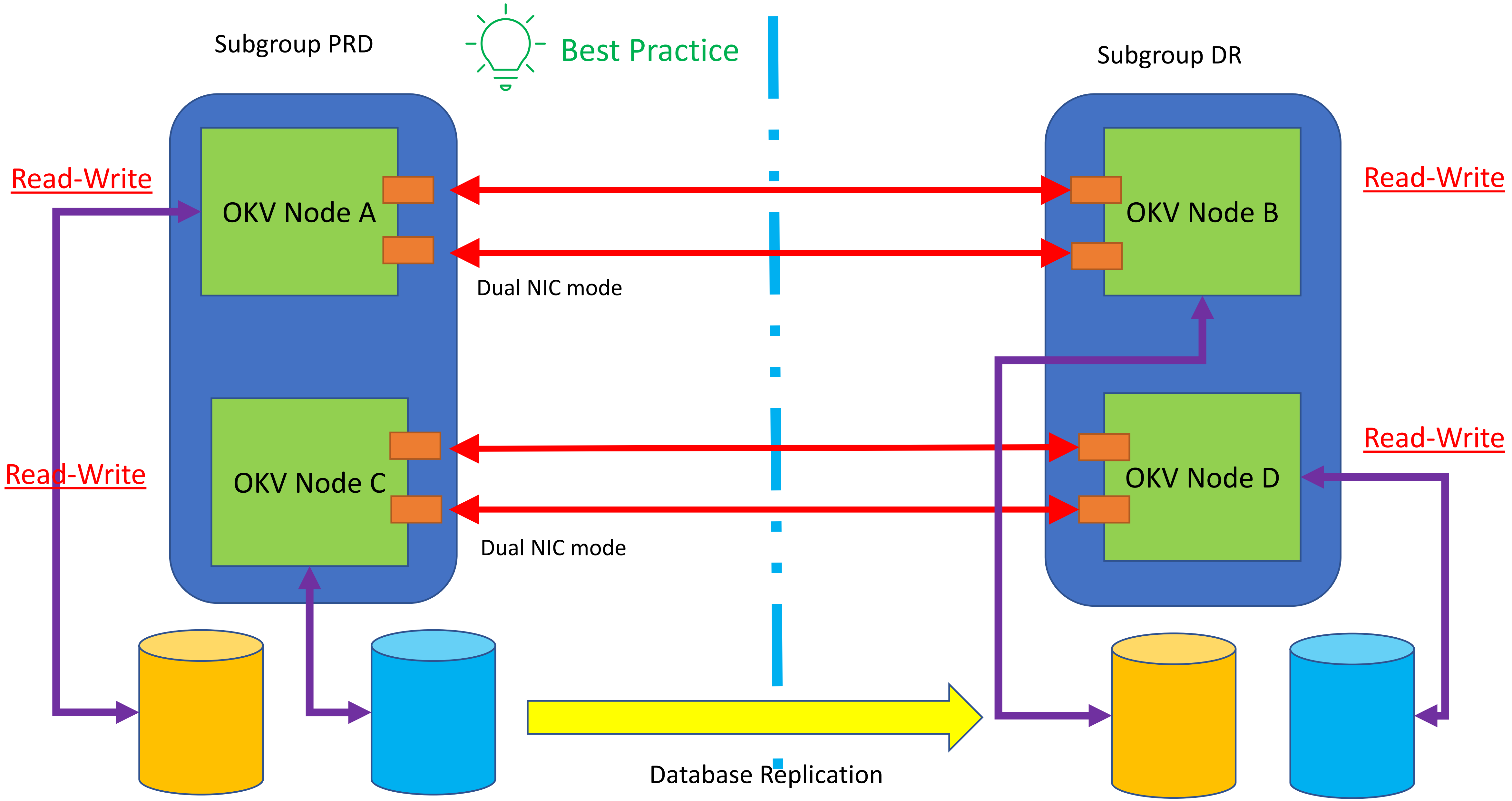
Oracle Cloud Infrastructure Vault

- Support **OCI only** workloads
- Oracle-Managed & Customer-Managed Encryption
- Software & HSM protected keys
- OCI Native
- Used in Exa@CC Gen2 – OKV integration for storing keystore passwords

Vault

Oracle Key Vault Architecture – overview and what we used

OKV – Multi-Master Cluster (MMC)



OKV – Multi-Master Cluster (II)

- Allows High Availability and Load Balancing for endpoints
- **Active-Active** architecture – endpoints traffic support in multiple DCs. No passive machines in cluster, which allows better resource utilization.
- Online scaling up/down. Maximum number of nodes in cluster => **16**
- **Online maintenance** capability for endpoints.
- **Local affinity for endpoints**. Scan List and Subgroups entities allows failover to local OKV node to avoid significant additional network traffic across data centers
- It is set of 2 node **read-write pairs**. Data is replicated across entire cluster, but read-write pair has synchronous replication set as priority. Primary/Standby databases should be attached to the same read-write pair.
- You can perform only one cluster change operation (such as adding, disabling, or deleting a node) at a time.
- **Maximum Disable Node Duration** – **very important** parameter in Cluster architecture
- **Read-only pairs** – for load balancing and scaling

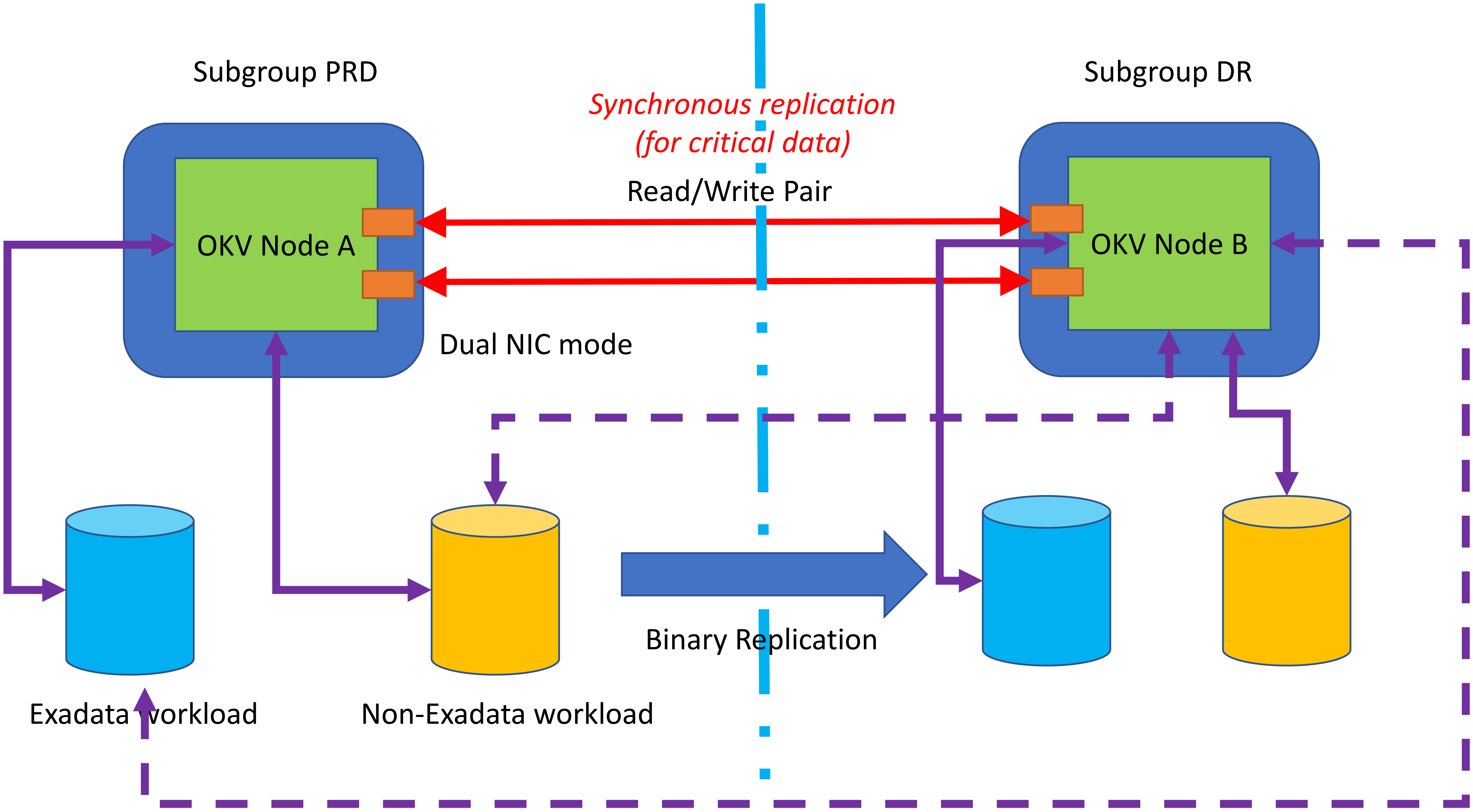
Architectural decisions & Technical Debt

TECHNICAL DEBT
I DON'T UNDERSTAND WHY IT TAKES SO LONG TO ADD A NEW WINDOW.
@VINCENTDNL

source

Not all projects start from scratch when you start working on them ☹

OKV 2-Node Multi-Master Cluster



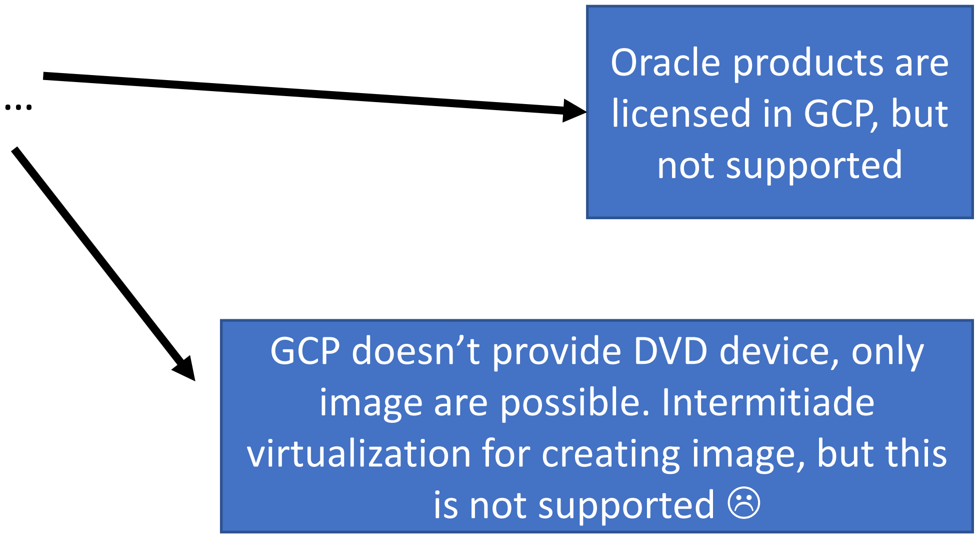
Architectural decisions – High Availability and Disaster Recovery

- We inherited **4 bare-metal servers** for host entire OKV ecosystem (no possibility to change numer neither type in resonable time). For **all enviornments**.

- Due to security requirements we cannot build one 4-node multi-master cluster for serving both production and non-production environments. Because we don't have requirement for non-extractable encryption keys from OKV servers, we decided to build 2x ***2-node multi-master clusters***, PROD + DR, DEV + UAT

- Nodes unavailability (both planned – upgrade and uplanned) are mitigated by using **pernament cache**. It is global setting for endpoints.

- Originally it was planned to install OKV in **Google Cloud**, but …



Oracle products are licensed in GCP, but not supported

GCP doesn't provide DVD device, only image are possible. Intermitiade virtualization for creating image, but this is not supported ☹

GCP still not suported (OKV 21.6 – 16th Oct 2023)

- Bare-metal servers used for avoiding latency problem between OKV and databases

OKV – 2-node MMC HA – what we learned

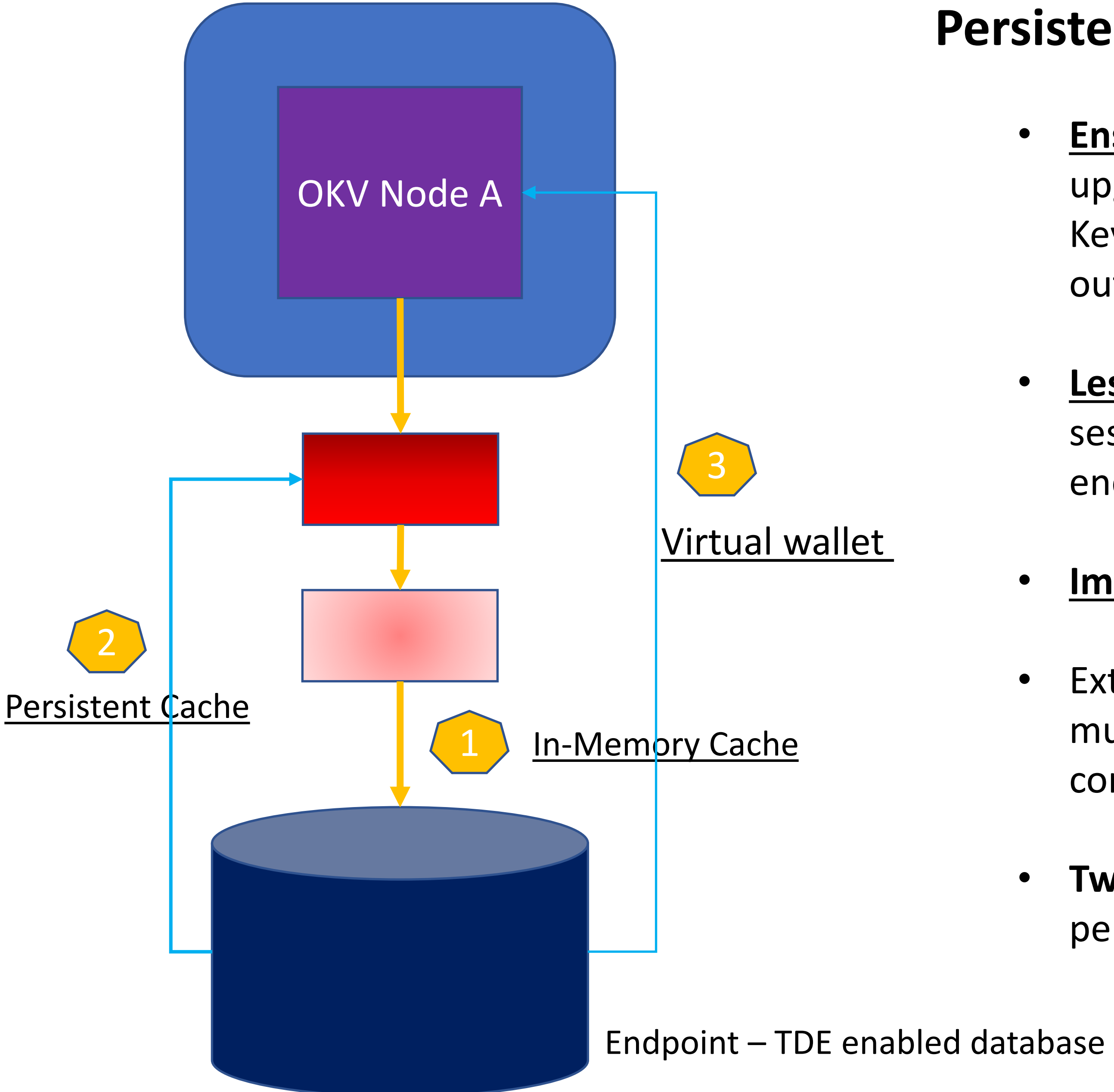
- **Maximum Disable Node Duration - MDND** (max. **240h**) is very important OKV parameter. Nodes are marked as „disabled" during maintenance activities (like os upgrade, okv upgrade)

- When single node fails remaining node in pair switches to **read-only mode**

- When single node fails it is marked as **disabled**. **If MDND passed it cannot be „reattached"** to OKV cluster. You have to reinstall OKV there and induct this node to cluster as fresh node.

- Standalone OKV cluster could be converted to cluster, however **1-node OKV cluster cannot be coverted back** into standalone OKV node

OKV – Persistent Cache concept



Persistent Cache benefits

- **Ensuring continous operation** of endpoints during upgrade, failover and other procedures that require Oracle Key Vault restart operation. No persistent cache enabled – outage for endpoints during operational maintenance.
- **Less load on the Oracle Key Vault server** when multiple sessions of a single database request the same master encryption key
- **Improved scalibility** of Oracle Key Vault
- Extractable attribute of TDE **master encryption keys** (**MEK**) must be set to true to enable persistent cache. Could be configured per single MEK.
- **Two modes possible** – contact OKV first or contact persistent cache fist

OKV - Reverse Migration

- ➢ Use case – when you have **read-only node** in OKV read-write pair (failure) and you have to **rotate MEK** and just rotate encryption keys and you cannot bring back quickly failed OKV node to have read-write pair.

- ➢ Best workaround for compromised keys (and single node in read-only mode) - migrate wallet from OKV to local TDE wallet (on ACFS for example and copy across data centers/availability domains for standby databases) and perform keys rotation

Steps

- ❖ Download wallet from OKV using okvutil tool on database server
- ❖ Create tde diectory on ACFS and move ewallet.p12 file to tde directory
  Oracle expects wallet file inside <wallet_root>/tde folder
- ❖ Change wallet related parameters
- ❖ Restart database
- ❖ Open wallet
- ❖ Perform tests to confirm encrypted data is available
- ❖ Create auto-login wallet
- ❖ Restart database and perform tests

Architectural decisions

- **System Auditing**

Splunk was company SIEM (Security Information and event management) solution.
We decided to integrate OKV audits with Splunk using Splunk Forwarder. OKV audit logs are stored in node’s syslog. Audit logs are replicated between nodes in OKV. Duplicates are filtered by Splunk universal forwarder and only use in case of source node failure. Main benefit is managability – one auditing system

- **System Monitoring**

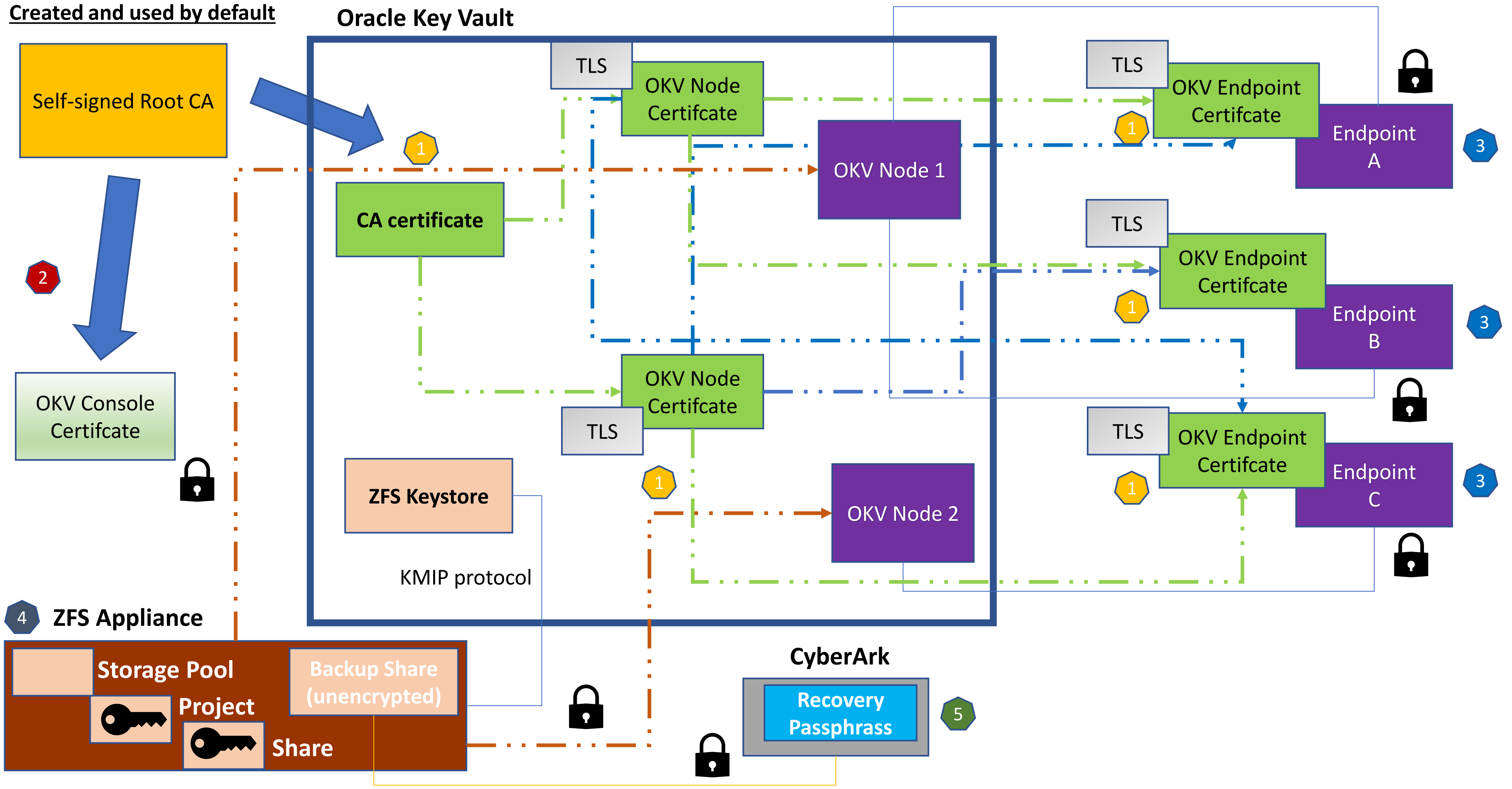
Oracle Enterprise Manager 13c was company solution for monitoring all Oracle related workload
(both on Exa@CC or non-Exa@CC databases). OEM integrated futher with incident and change management tool -> Service Now.
Bug 29678875 : INTEGRATION OF ORACLE KEY VAULT WITH OEM 12C/13C -> ***Still (since 2019) not implemented*** ☹
We implemented Splunk for resource usage monitoring and email alerts. OKV Console is main place for system monitoring.

Architectural decisions – central keystore

Central „keystore” in environment

- Second component with keystore/wallet is ZFS appliance
- ZFS appliance role in environment is to take care of all database backups

Oracle Key Vault – encryption in environment



Oracle Key Vault – encryption in environment

We have identified five components which could be rotated

1 OKV CA certificate, OKV Node certificate, OKV endpoint certificate (endpoint host)

2 OKV Console certificate

3 Database endpoint encryption keys (rekey manually or part of Master Encryption rotation)

4 Oracle ZFS Storage Appliance keystore (used for projects and shares in ZFS which are used for database backups)

5 CyberArk. It stores Recovery Passphrase – critical component

Legend

— · · ▸ OKV backups are stored in OKV

— · · ▸ Encryption-in-transit between OKV components (TLS) – active connection

— · · ▸ Encryption-in-transit between OKV components (TLS) passive connection

—— Use – Store encryption key relation

—— Use Recovery Passphrase

Oracle Key Vault – encryption components rotation

You need to know

- Rotation is required for them as when certification validity period passed communication between OKV servers and endpoints will be disabled – outage for all encrypted components using OKV – databases and ZFS appliance

- There is no way for monitoing rotation progres. OKV node certificate rotation took 6 days ☹

- OKV provides possiblity to put Intermediate CA certificate issued and signed by Company CA. We used Keyfactor as central certification issuer.

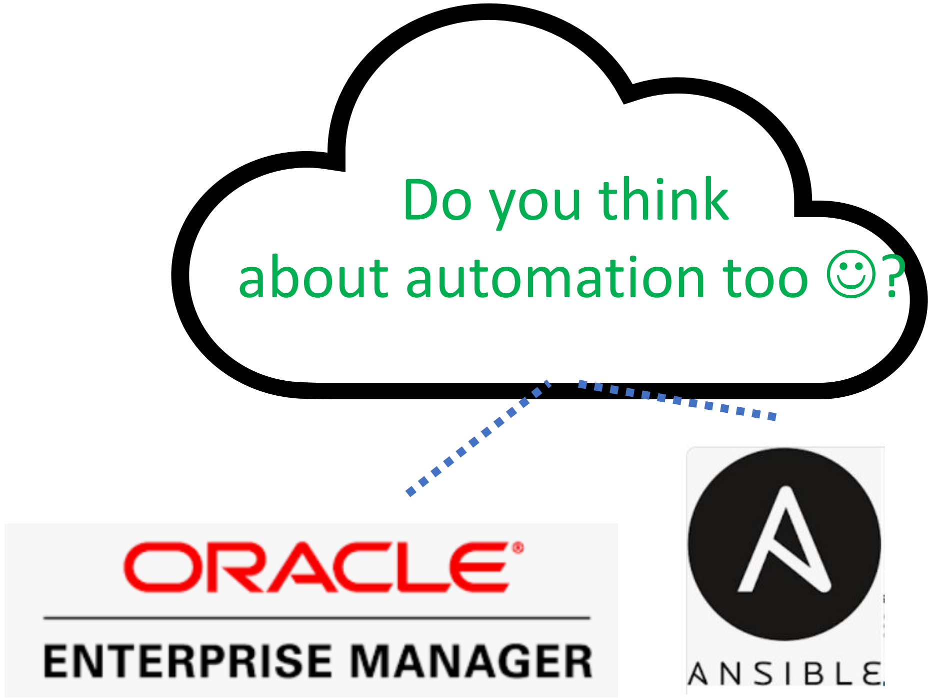
- Oracle enforces certificate validity intervals (min and max). You cannot set outside interval. Certificate simple will be rejected. We found this

KEYFACTOR
Where digital trust happens

OKV and components rotation

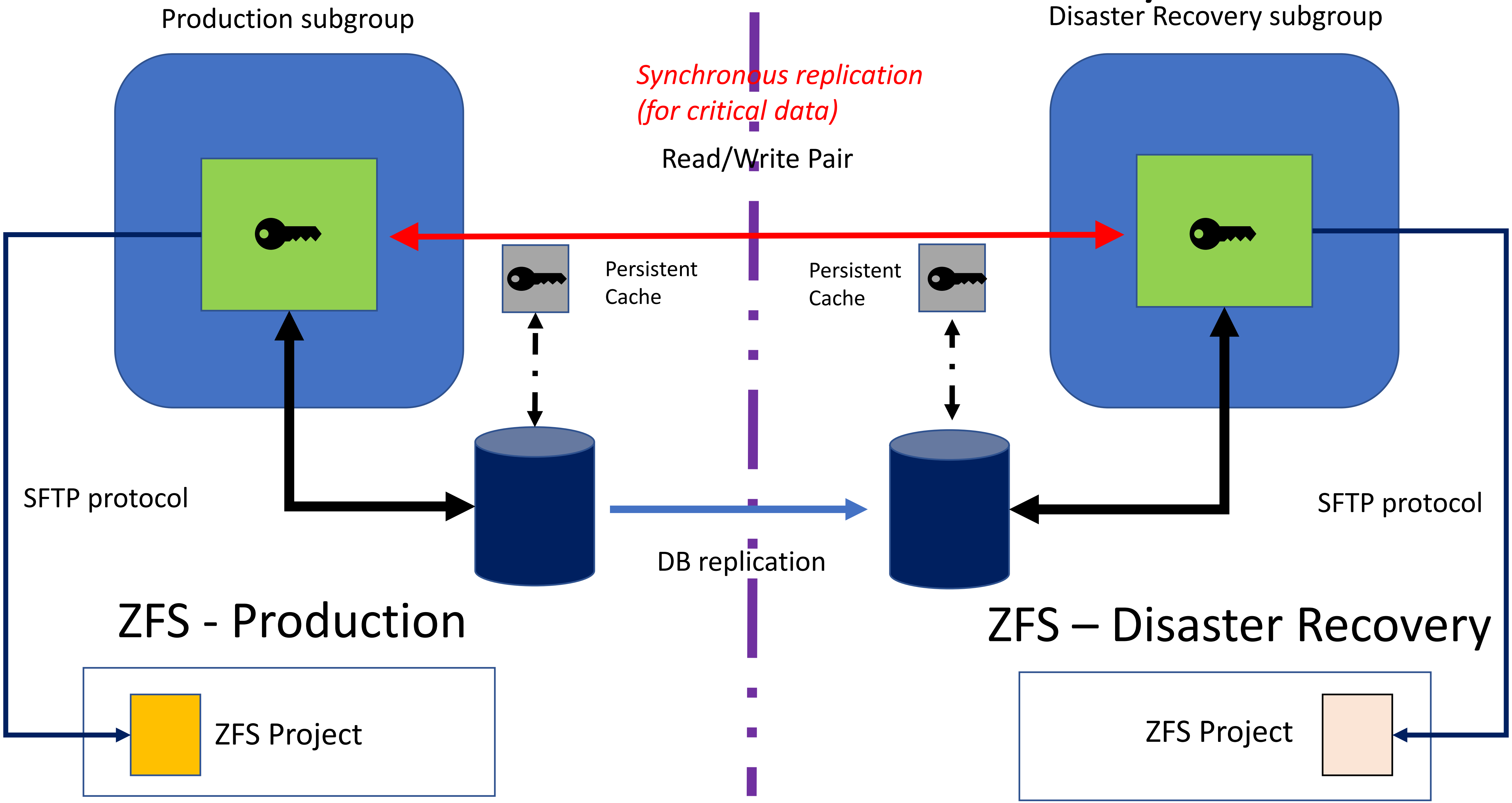
OKV is central key management system, but ……

*You can rotate the TDE master encryption key of the database **<u>only from the database</u>** using the Administer Key Management Set Encryption Key commands. You cannot initiate the TDE master encryption key rotation centrally from the Oracle Key Vault management console.*



Do you think about automation too ☺?

Architectural decisions – resiliency



Architectural decisions – resiliency

Why and How?

- **Local OKV backups not needed**. They have limitation - only last FULL and all incremental cumulative backups are stored
- Daily „local” **remote backups** for each OKV node
- We are using backups for both primary and physical standby database
- Separated (and **not replicated !!!)** ZFS projects for each OKV node (one in each data canter).
- ***Ransomware attack*** is not going to destroy backups as OKV backups are stored in 2 separated locations.

OKV Backup & Restore – what we learned

- OKV backup could be only restored using recovery passphrase (recovery passphrase **valid during backup time**).
  OKV backup-recovery passphrase mapping should be stored in safe place. We used CyberArk for this.

- Maximum life of backup is **1 year**. Checks during restore reject older backups.

- Oracle Key Vault encrypts all backed data. So even we are using **unencrypted share on ZFS data is protected**.

- **Restore is only possible to single server**. We cannot restore entire OKV from backup to existing Mulit-Master Cluster. Restore means outage for entire environments and means build Multi-Master Cluster again. For existing cluster unpair step will be required.

- Restore from OKV backup only if encryption keys availability and consistency cannot be satisfied by remaining nodes in cluster.

Architectural decisions – scaling

- Single OKV node is capable for serving **100 endpoints**
- Oracle **RAC database** is **counted as single endpoint** in scaling exercise.
- OKV Cluster could be extended up to **16 nodes**
- Scaling-up **doesn’t automatically load balance** endpoints. Try to build cluster upfront.
- OKV Nodes are grouped in subgroups to allow select local OKV in case of failure current node.
- **Per database limit** – single database might check the **MEK 1000s** of times per second (all of these operations are counted against this limit – heartbeat, new process, startup, redo logs switch, backup, multi-tenant, Data Guard etc.)

Tests and Fool Theory

It's the economy, fool! → Catenaccio, fool! → Tests, fool!

James Carville, 1992, Washington (USA)

Helenio Herrera , 1960, Milano (Italy)

Unkown IT manager, 1990+

World Cup 1982

Last medal place (3rd) for Poland.

Tests help verify your assumptions.
In software development they call it ***Test-driver Development*** *(first test, implementation later and final test)*

World Cup 2006

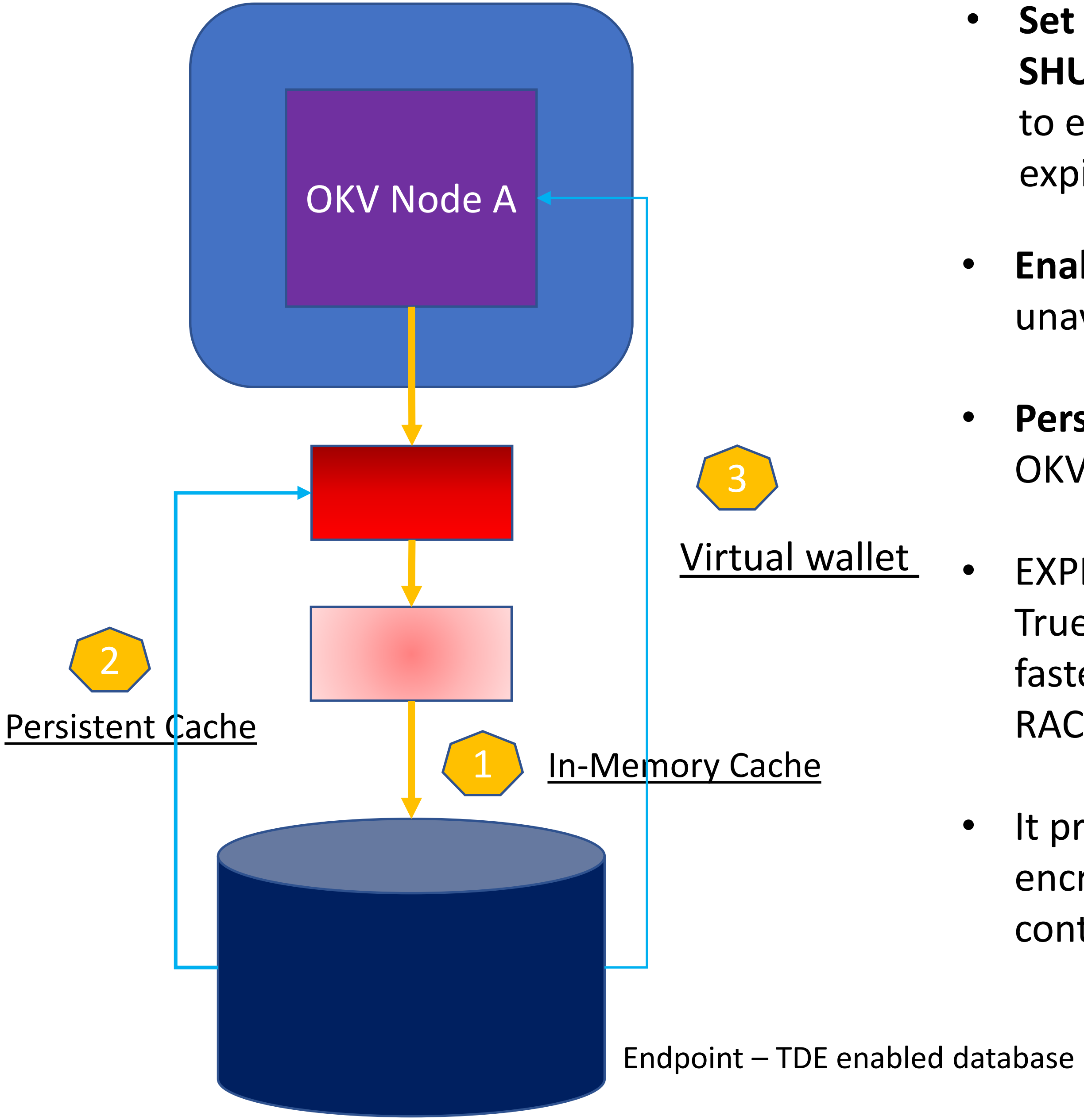
Modern evolution of this system is used
by most best football teams during World Cups till now !

Source => Wikipedia

Test – OKV HA for database

Description	Test Plan	Expected outcome	Test outcome	Notes
OKV HA for database – single local node failure OKV is configured as 2-node cluster with one read-write pair. Database has been registered in local OKV node and encryption key replicated to remote node	1. Perform tests to confirm database works as expected. 2. Database with MEK migrated to OKV. 3. Shutdown local OKV node. 4. Perform tests to confirm database works as expected. 5. Restart database. 6. Perform tests 7. Bring up local OKV node 8. Perform tests	Database should be available during local OKV node unavailability. Database should be fully available after restart. Remote OKV node should switch to read-only restricted mode and returns to read-write as soon as remote OKV node bring up.	Database remains available during local OKV nodes' unavailability. Remote OKV node switched to read-only restricted mode and returns to read-write after bring up local OKV node.	Persistent cache is required. *EXPIRE PKCS11 PERSISTENT CACHE ON DATABASE SHUTDOWN* is important parameter if we want to have fully available database when local OKV is no available.

Persistent Cache – What we used/set



- **Set EXPIRE PKCS11 PERSISTENT CACHE ON DATABASE SHUTDOWN parameter** (possible only in OKV console) to ensure PKCS#11 persistent cache automatically expires upon shutdown of the endpoint database
- **Enabled persistent cache for all databases –** limited unavailability SLA for databases
- **Persistent cache first mode** – no additional delays when local OKV is not available
- EXPIRE PKCS11 PERSISTENT CACHE ON DATABASE SHUTDOWN = True for all databases. Database are RAC databases and we faster brings missing OKV node than probability of crash of all RAC database instances.
- It provides **protection for stealing databases**. When enabled, encrypted data will not be available for database without contacting OKV.

Test – TDE Master Encryption rotation & rekey

Description	Test Plan	Expected outcome	Test outcome	Notes
TDE Master Key Encryption rotation & rekey We are usning TDE isolation mode for databases. All of them are multitenant.	1. Perform tests to confirm database works as expected. 2. Change MEK on root level. 3. Change MEK in pluggable databases. This triggers rekey operation for all tablespaces in pdb. 4. Perform tests to confirm database works as expected. 5. Confirm using metadata in database and OKV new MEK is created.	New Master Encryption Keys are generated and used for generating new tablespace level keys. Tablespace encryption keys are rotated. Changing MEK in pdb triggers rekey operation for tablespace level keys automatically.	As expected.	When quering MEK in OKV console all MEK keys have hard coded prefix -> 06.

Oracle multitenant modes – keystores’ management

❑ Multitenant modes for the management of keystores

➢ **United mode**
  - Enables customer to configure one keystore for the CDB root and any associated united mode PDBs
  - United mode operates much the same as how TDE was managed in an multitenant environment in pre 18c release
  - It doesn’t mean all pluggable and root shares the same Master Encryption Key

➢ **Isolated mode**
  - Enables customer to create both keystores and TDE master encryption key in an individual PDB
  - PDB can have diffirent keystores types (software keystores, Oracle Key Vault)

❑ Isolate mode and HSM has significant performance problem and is not recommended by Oracle in multitenant infrastructure. It is more HSM design limitation.
We did not have requirement for using HSM. Uff ☺

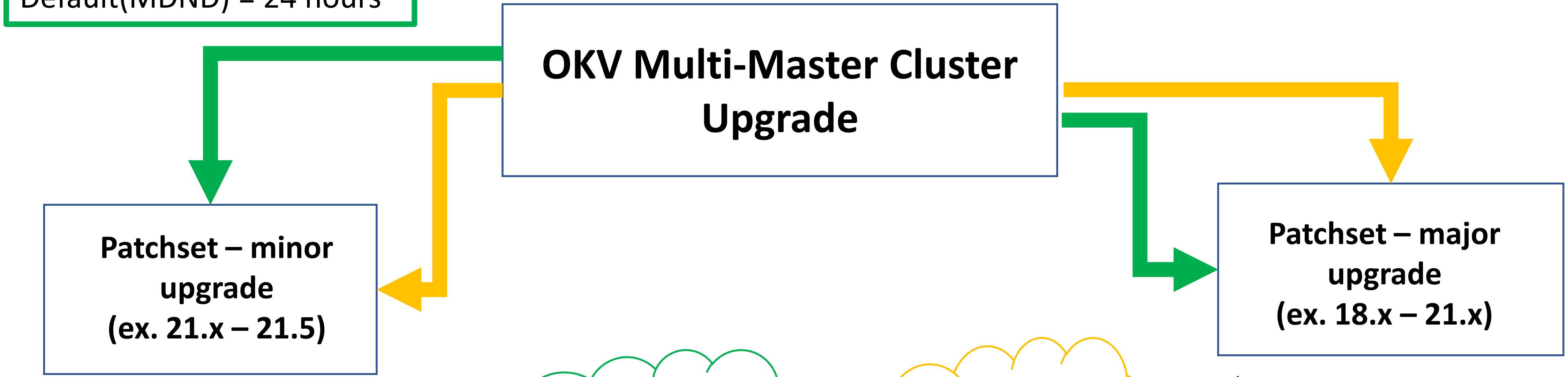
❑ United mode allows easier operations in environment – less work needed

Test – OKV Upgrade

Description	Test Plan	Expected outcome	Test outcome	Notes
OKV 2-node MMC upgrade from 21.5 to 21.6 version	1. PreUpgrade checks. 2. Perform tests to confirm database works as expected. 3. Disable first OKV node 4. Upgrade 1st node using newest OKV ISO image. Enable it. 5. Disable second node. 6. Upgrade second node using OKV ISO from point 4. 7. Upgrade endpoint software. 8. Perform tests to confirm database works as expected.	Online upgrade in rolling fashion. Online software upgrade for RAC databases.	OKV cluster upgrade is online. Endpoint software upgrade requires database restarts (19c was our version) Custom OS configuration – repeat modification!	.

Max(MDND) = 240 hours
Default(MDND) = 24 hours

OKV upgrade (1)



OKV Multi-Master Cluster Upgrade

Patchset – minor upgrade
(ex. 21.x – 21.5)

Patchset – major upgrade
(ex. 18.x – 21.x)

- ✓ Two-phase upgrade
- ✓ OKV cluster upgrade online with persistent cache – first phase
- ✓ Endpoint software upgrade with outage for endpoint (even for RAC databases) – second phase
- ✓ Rolling upgrade approach

Increase MDND!

Rekey required for upgrade (if extractable attribute = false) !

- ✓ Two-phase upgrade
- ✓ OKV nodes upgrade online with persistent cache – first phase
- ✓ Endpoint software upgrade with outage for endpoint (even for RAC databases) – second phase
- ✓ Rolling upgrade approach
- ✓ No delays between phases. Old endpoints software doesn't work with upgraded nodes.

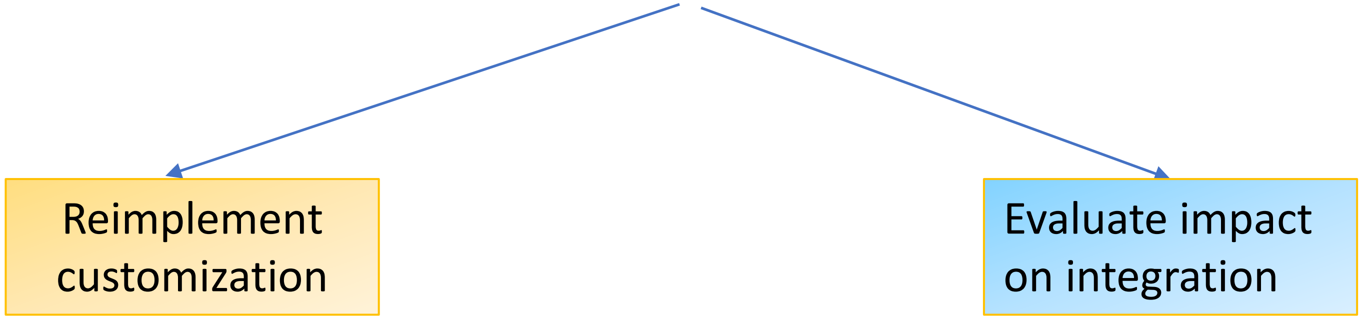
OKV upgrade (2)

We learned …..

Oracle Database 21c is first release which allows OKV upgrade without downtime because it allows dynamic loading of PKCS#11 library available when database is running

OKV Upgrade – What we learned

□ **Integration** – it’s nearly certain some customization in OKV will be required (for example access management with CyberArk) and cause additional steps in upgrade procedure



Reimplement customization

Evaluate impact on integration

□ **Downtime** – until 21c version required, but good news is you could split downtime actions in bulks

□ No one-timeoff patches – delivered only as patchsets (new ISO)

□ **“Standby first”** upgrade method is supported

□ **No new OKV features** could be used if you are in **mixed configuration** (21.5 – 21.6 cluster).
You have to have all nodes upgraded.

□ For not very deep OS modifications Oracle Support is happy to **approve OKV customizations**

□ Upgrade time for single node is simiar like for fresh installation => around **6 hours** on bare-metal using iso mounted using ILO

Encryption Keys Migration from Wallet into OKV

High Level Plan

- Setup $OKV_HOME (Wallet Root) for each database endpoint
- Download RESTful Service Utility from OKV (accessible via HTTP)
- Update okv_wrapper_utility
- Update OKV client configuraiton file – okvrestcli.ini
- Create Wallet, Endpoints and install endpoint client software => OKV Client
- Copy current TDE Wallet to $OKV_HOME/tde
- Update Wallet
- Enable auto-login property for wallet
- Update database initialization parameters
- Migrate encryption keys
- Update cloud registration configuration file (CREG) to allow smooth support from EXA@CC Gen2 cloud tooling
- Verify wallet status and verify databases work correctly

Encryption Keys Migration – What we learned

OKV with RBAC (Role Based Access Control) enabled requires two OKV user credentials to perform keys migration.

Oracle note *„Migration of File based TDE to OKV Gen 2 ExaDB-C@C Using Rest (Doc ID 282857.1)* is good starting point to produce automation scripts, but adjustment could be required.

In our case we have single regular pdb in container database, but if you have more than 3-4 pluggable database it could cause some false alarms in OKV related to hearthbeat. By default heartbeat is send in one batch, so it takes longer. Solution (available in Oracle 23c) is configuring **HEARTBEAT_BATCH_SIZE** parameter to reduce batch size.

Automated migration is **quite fast** – around 5-10 minutes for database (replication confirmation is main consumer)

OKV – Learning Resources

1. Oracle Key Vault FAQ (MOS 2372010.1)
2. Primary Note For Oracle Key Vault (MOS 2120572.1)
3. Oracle Key Vault RESTful Services Administrator's Guide
4. Oracle Key Vault Installation and Upgrade Guide
5. Oracle® Key Vault Readme Release 21.5 F56594-01
6. Commercial National Security Algorithm Suite – Wikipedia
7. MySQL :: Security in MySQL :: 6.4.8 Using the keyring_okv KMIP Plugin
8. Mapping LDAP Groups in Oracle Key Vault
9. What Is FIPS 140-2? (trentonsystems.com)
10. https://www.Oracle.com/assets/cloud-licensing-070579.pdf
11. 17. SR 3-31875650941: Oracle Key Vault deployment with Exadata Cloud at Customer
12. Install Oracle Key Vault
13. Oracle Lifetime Support Policy for Technology Products Guide
14. Alert: Exadata Cloud: "OPatch Util Cleanup" Removed all the TDE Database Wallets From the "/var/opt/oracle/dbaas_acfs/<DB_NAME>/*_wallet/*" Location (Doc ID 2733960.1)
15. Where are the TDE and DB wallets backups on ExaCloud machines? (Doc ID 2733403.1)
16. Backup and Restore Operations (oracle.com)
17. Migration of File based TDE to OKV for Gen 2 ExaDB-C@C Using REST (Doc ID 2828575.1)
18. Managing Encryption Keys on External Devices (oracle.com)
19. Understanding non-extractable keys with OKV
20. Oracle Security Blog
21. Ask Tom Office Hours
22. DB Security – Key Vault (Live Lab)

Summary

- Check you assumptions & design. You could learn a lot and adjust them just in time. It won’t always work with what you’ve been doing before ……. And even if it is the IT world that changes very quickly. Test-driven Development strategy could help you.
- Cooperate with your vendor – there is (nearly) always space for flexibility in appliance. Black Box? No, rather Grey Box. Product Managers are not behind a firewall completely.
- Be creative – lack possiblity of achieve best practice is sometimes not hard blocker.
- Oracle Key Vault is product which could help you meet security controls in large environments
- OKV doesn’t follow all new features & trends very rapidly, but we appreciate stable approach
- Oracle Key Vault is software appliance, but it doesn’t live alone in environment. Adapting to integration is not an invention, but a necessity. Very often you have stack not from one vendor only ….
- Test & Adjust your operational procedures – some of them should be adjusted after implementing OKV (like for example PDB cloning between container databases)

Thank you ☺ !