深入了解Oracle Key Vault密钥保险箱(OKV)

公益讲座11：00准时开始，请大家先浏览云技术微信公众号技术文章。资料会在各群同步发布，已入群客户请勿重复入群！

20-21

数据库和云讲座群

甲骨文云技术公众号

B站专家系列课程

基于 Oracle 数据库
免费企业数据健康检查

- 及时了解数据库健康状况，发现并解决潜在问题
- 维护数据库系统良好状态，保护数据资产的安全
- 提升数据库性能、稳定性和安全性，降低业务风险

免费咨询热线：
400-699-8888

* 活动最终解释权归甲骨文公司所有

深入了解 Oracle Key Vault 密钥保险箱 (OKV)

甲骨文技术公益课 - 数据库专场

2023 年 9 月 8 日 11:00

线上直播

Benson Zhong

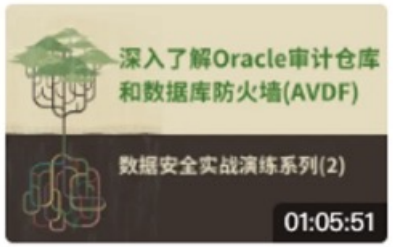
主页 动态 投稿 245 合集和列表 15 收藏 0

TA的合集和视频列表 > 数据安全实战演练系列

2个视频 | 8-4更新

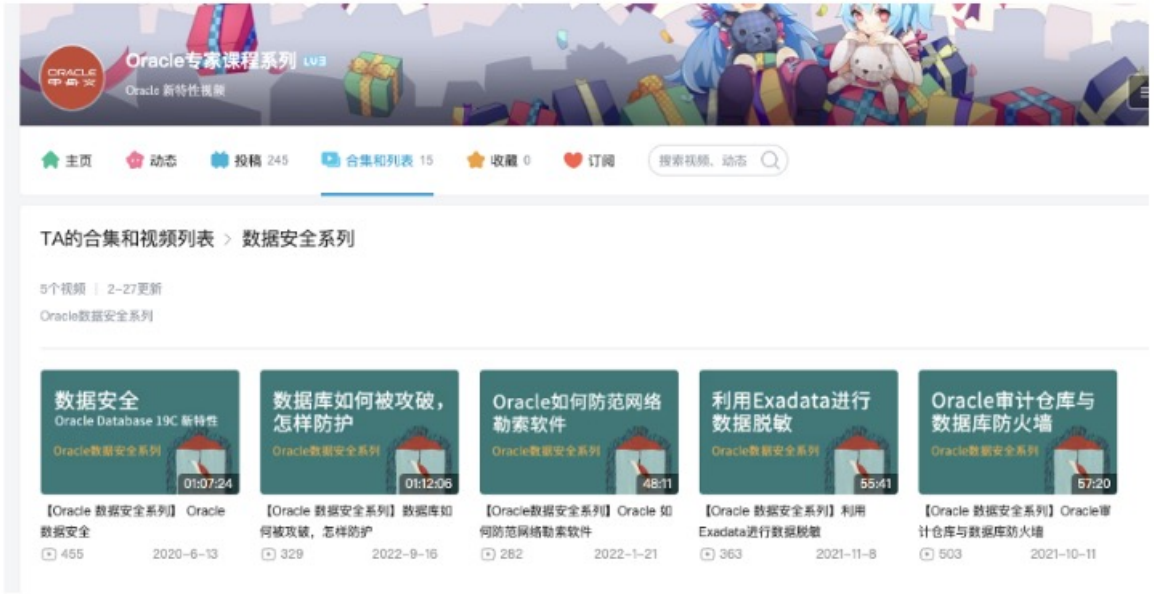
【Oracle 公益课堂 】Oracle透明数据加密(TDE)

617 6-30



【Oracle 公益课堂 】深入了解Oracle审计仓库和数据库防火墙

438 8-4



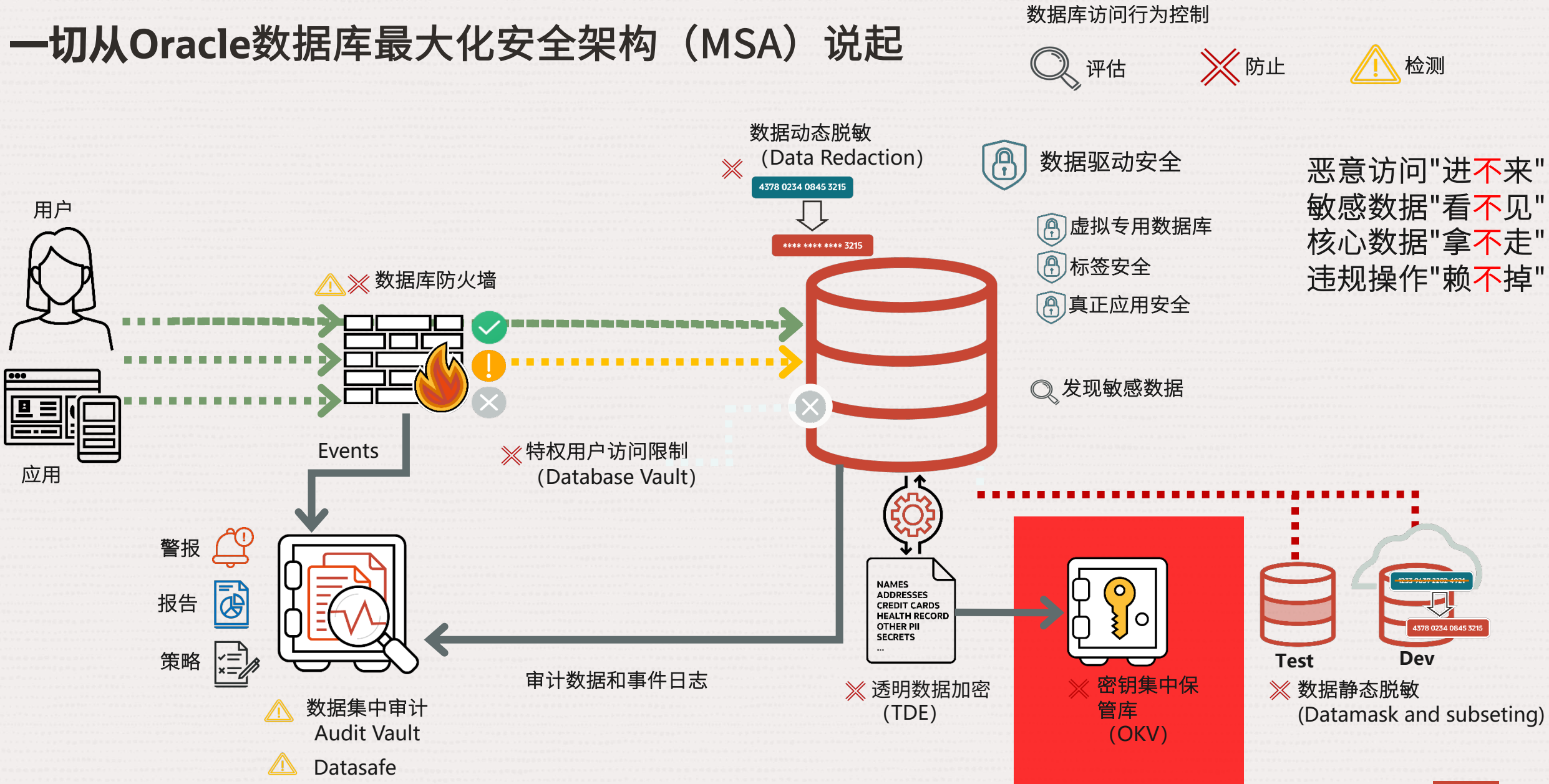
内容

深入了解Oracle Key Vault密钥保险箱(OKV)

- OKV概述
- OKV应用场景
- OKV动手演示
  - OKV界面以及概念的介绍
  - OKV管理TDE Master key
  - OKV管理数据库密码
- Q/A

OKV概述

一切从Oracle数据库最大化安全架构（MSA）说起

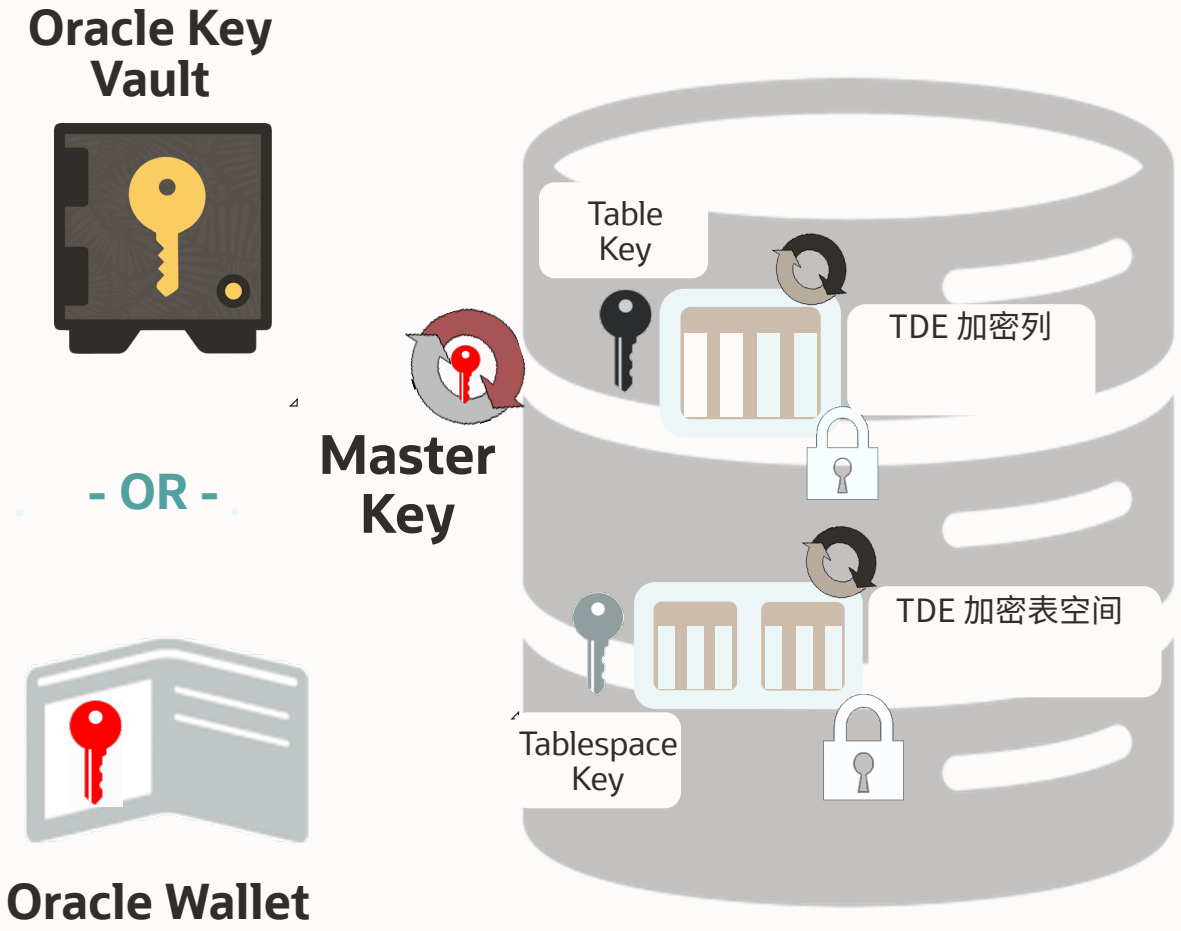


TDE关键架构

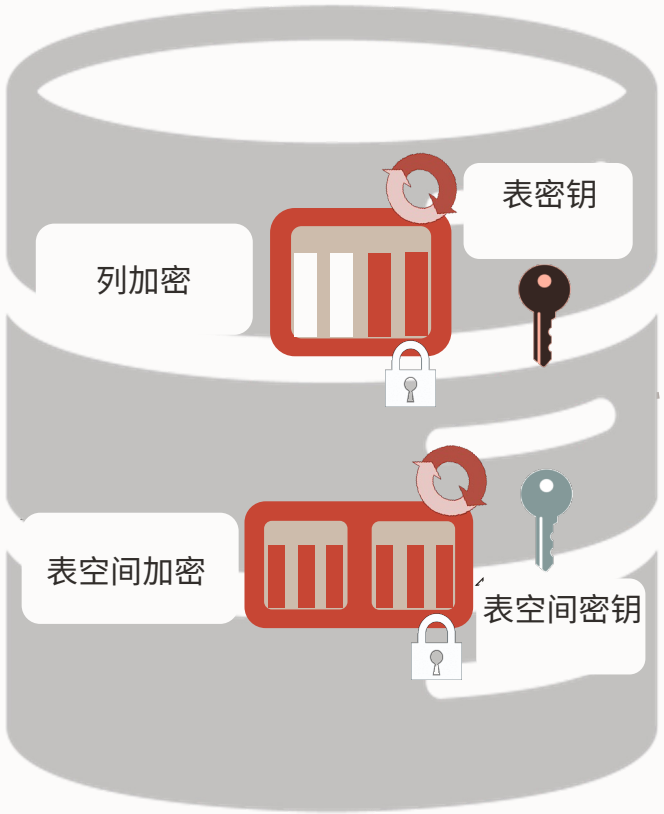
数据加密密钥由TDE自动创建和管理

主加密密钥对数据加密密钥进行加密

主密钥通常存储在Oracle钱包或Oracle密钥库中



Oracle透明数据加密--架构及密钥管理

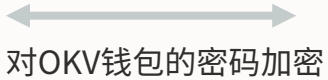


主密钥

密钥库文件keystore

· OR·

Oracle密钥保险库



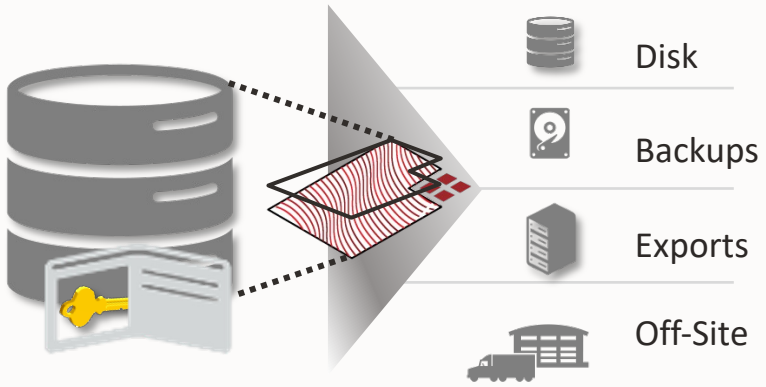
对OKV钱包的密码加密

第三方加密机

· OR·

第三方加密机

使用透明数据加密加密静态数据



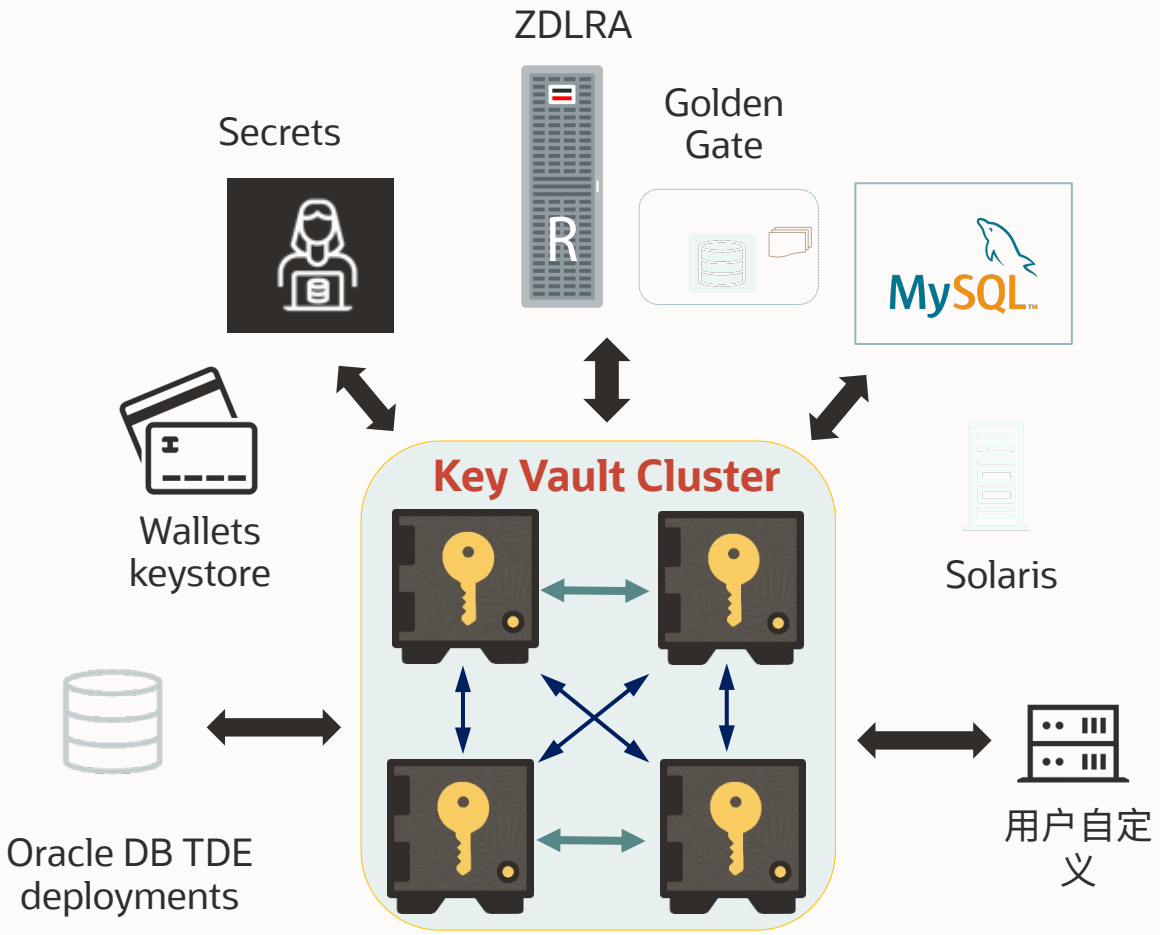
- 加密表空间或列
- 无需更改应用程序
- 非常低的性能开销
- 在线/离线迁移选项
- 使用钱包或 Key Vault 进行密钥管理
- 与 Oracle 技术集成

Exadata, Compression, ASM, Data Guard, GoldenGate, DataPump, Multitenant

Fusion Applications, eBusiness Suite, PeopleSoft, JD Edwards, SAP, …

阻止对任何地方的静态数据的带外访问

用于密钥和机密管理的 Oracle Key Vault



管理数百万个端点的密钥/秘密

- 在线访问和存档
- 针对 TDE 主密钥管理进行了优化
- Oracle 系列端点
- 适用于 C、Java、REST 的自定义端点的 SDK

企业级别保护

- 持续可用性和可扩展性
- 具有全局一致性的快速本地访问
- 使用 REST API 实现自动化
- 本地和云数据库
- 使用 OCI 映像快速部署
- Microsoft® Active Directory支持
- 流行的 HSM 作为信任root

OKV专为高可用性和极强的可扩展性而设计

存储和管理数千个数据库的加密密钥/钱包

Key Vault 节点在专用硬件上本地部署，或在 OCI 市场的云中部署

通过多主集群提供持续可用性

- 在一个集群中最多部署 16 个节点
- 用于本地访问和全局一致性的全连接节点

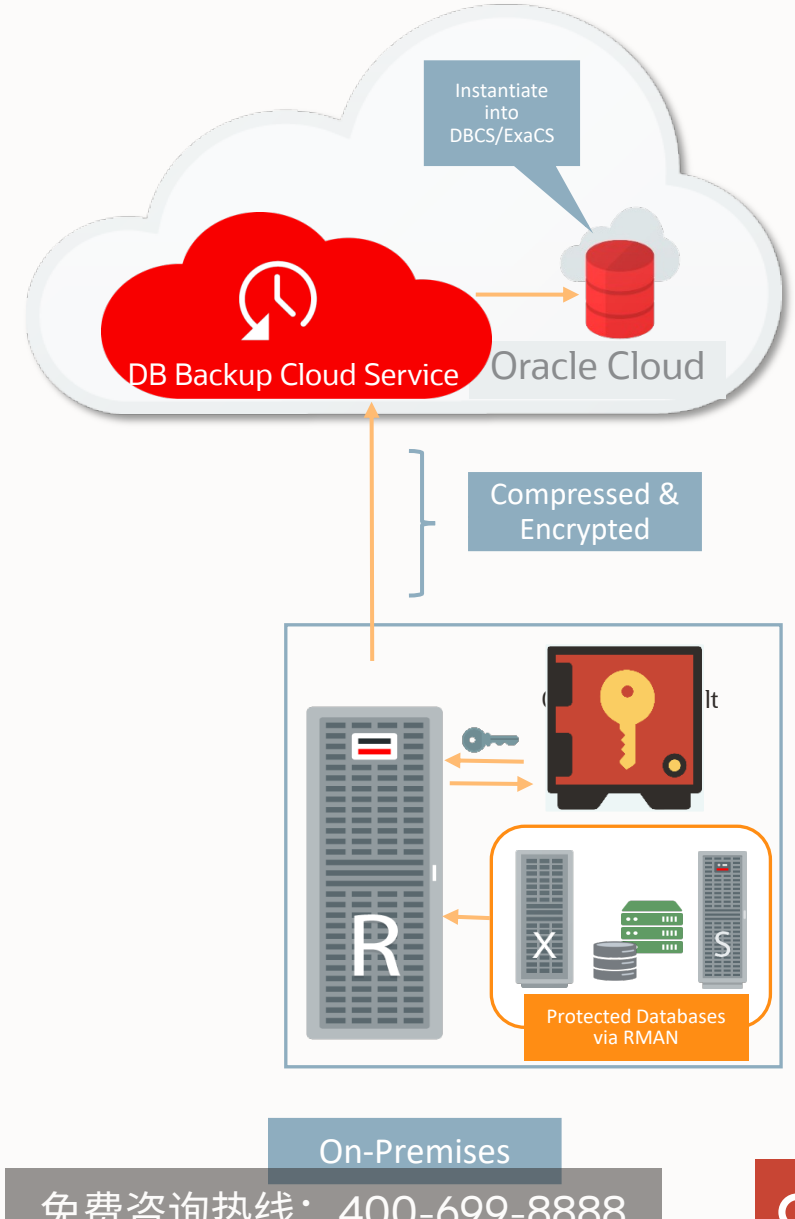
OKV进行 ZDLRA 归档加密

在 Oracle 数据库备份云服务中存储备份

- 利用由 Oracle 管理的经济高效的云存储层，将选项扩展到本地磁带之外
- 消除磁带存储服务

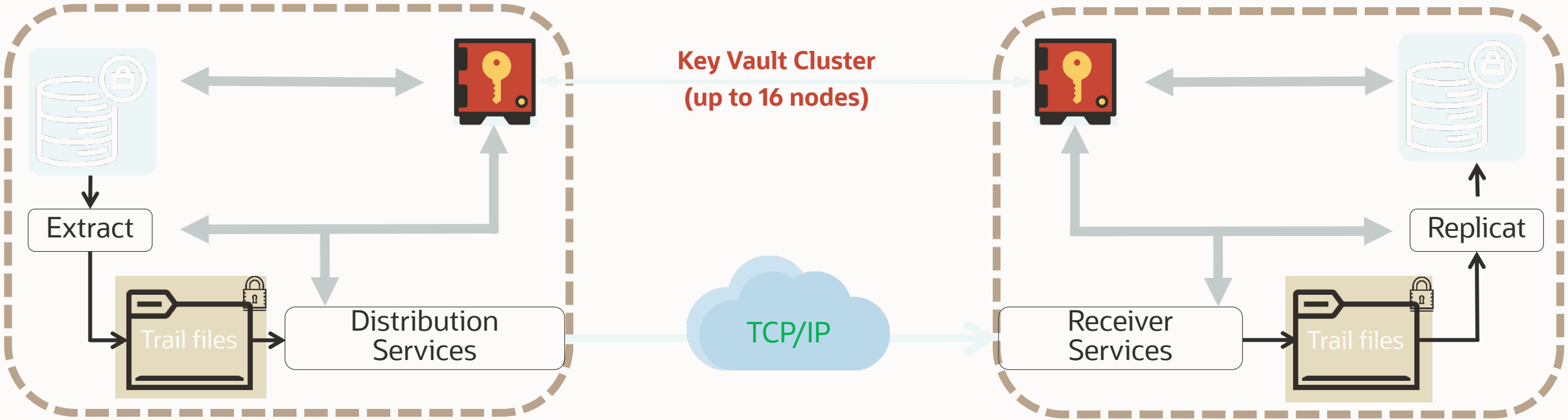
通过直接从云备份轻松配置云数据库，加速数据上云

- 存档备份已加密
- 使用 Oracle Key Vault 进行密钥管理



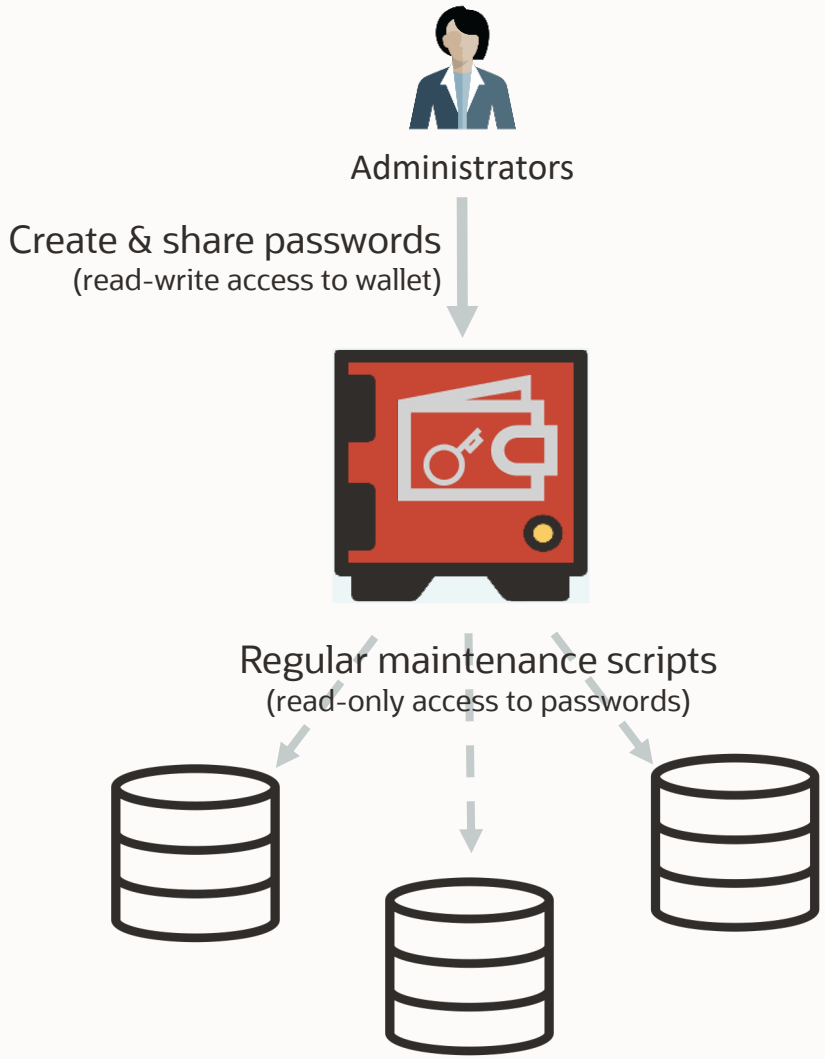
OKV管理Oracle GoldenGate trail file key

- Trail file加密主密钥与加密数据分离
- 绝对透明 – 无需更改应用程序，既定工作流程
- 完整的密钥生命周期管理，包括 密钥轮换，密钥过期
- 支持自带密钥 (BYOK)



使用OKV进行密码管理

- 集中创建和轮换密码
- 管理员授予或撤销端点对密码的只读访问权限
- 按需获取密码
- 端点主机上的零密码足迹
- 无需人工干预的更强大的密码
- 使用 REST API、C-SDK 或 Java SDK 轻松编写脚本



OKV自动化 API

用于设备自动化的新外观 RESTful API 接口包括

- 服务器管理
  - Endpoint部署和管理
- 访问管理
  - 管理endpoint组和钱包
  - 促进密钥和秘密的安全共享
- 安全对象
  - 密钥和机密生命周期管理
- 监控
  - 服务器运行状况和配置监控
- 备份还原
  - 自动管理远程目的地的备份

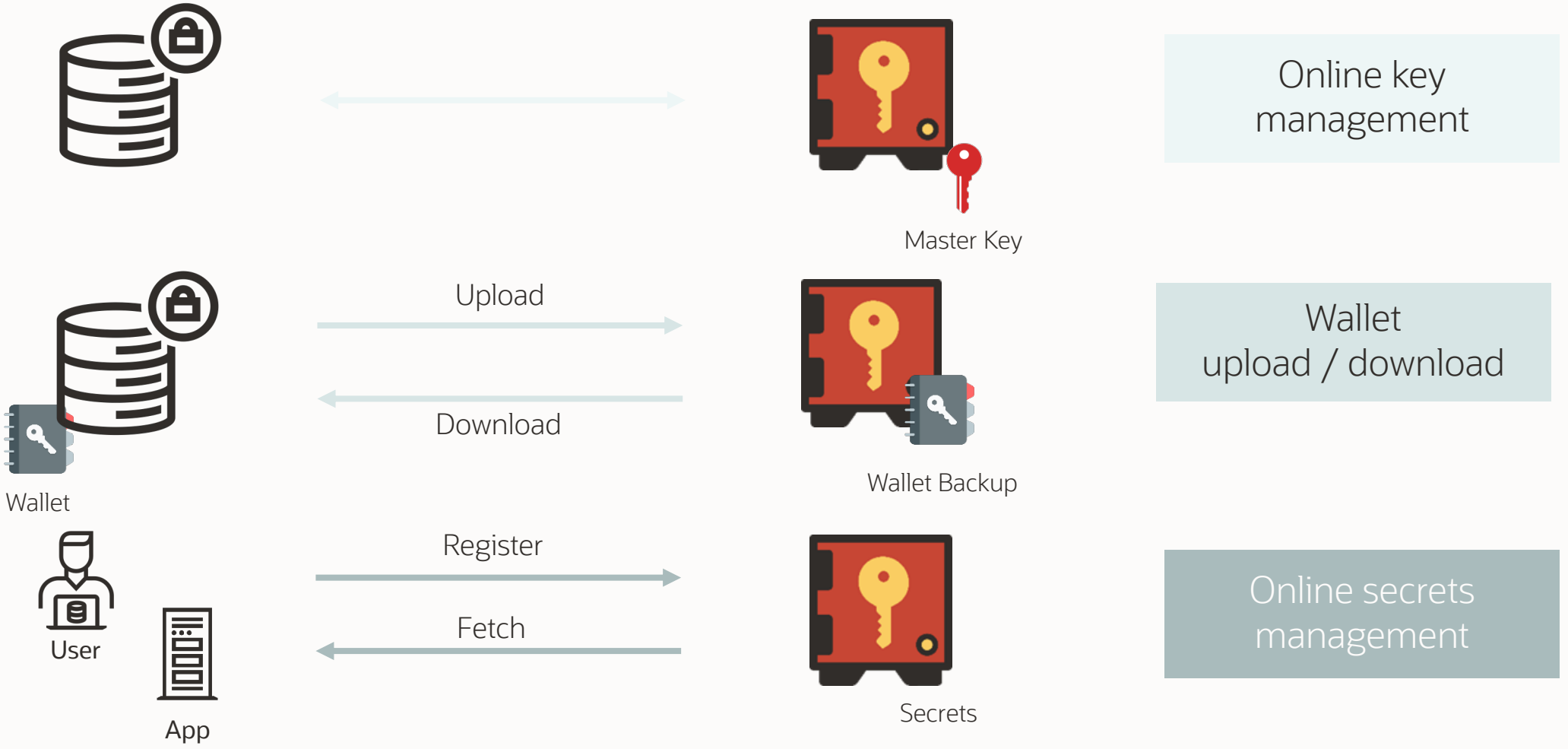
Get server status

```
$ okv server status get
{
 "result" : "Success",
 "values" : [ {
  "uptime" : " 1 day, 7:50 HH:MM",
  "freeSpace" : "90%",
  "backupStatus" : "Successful backup done today",
  "alertsRaised" : "1"
 } ]
}
```

Or just the uptime

```
$ okv server status get | ./jq .values[].uptime
" 1 day, 7:50 HH:MM"
```

OKV Key Use Cases

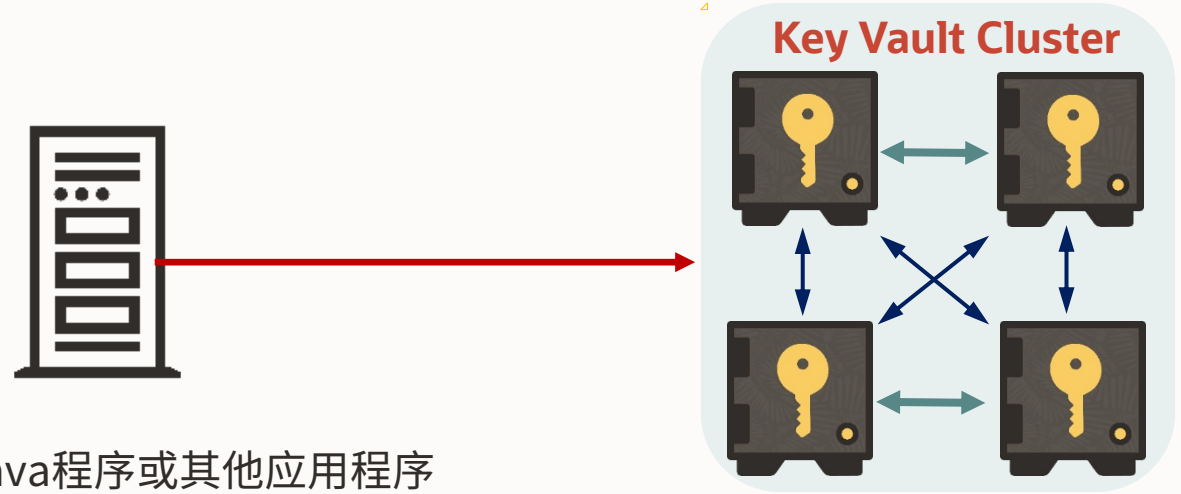


OKV密码管理工作流程

1. 在程序服务器上配置密钥保险箱的连接配置。
2. 为程序或数据库端创建endpoint。
3. 把密码和密钥通过endpoint上传到密钥保险箱。
4. 上传过程需要提供一个密码和密钥的locate名字，后面是通过这个名字取下密码和密钥。

OKV为自己程序管理密码或配置文件(无需修改程序代码)

把用户密码或整个配置文件上传到OKV



1. 通过定义的应用程序找到UUID。
2. 通过UUID找到password或配置文件。
3. 把真实password替换或使用新配置替换。
4. 启动应用程序
5. 把真实的密码替换回去或删除新的配置文件

```
<description>JDBC Password</description>
<param-name>jdbc.password</param-name>
<param-value>Oracle_Key_Vault_Replace_Password1</param-value>
```

```
<description>JDBC Password</description>
<param-name>jdbc.password</param-name>
<param-value>abc123487</param-value>
```

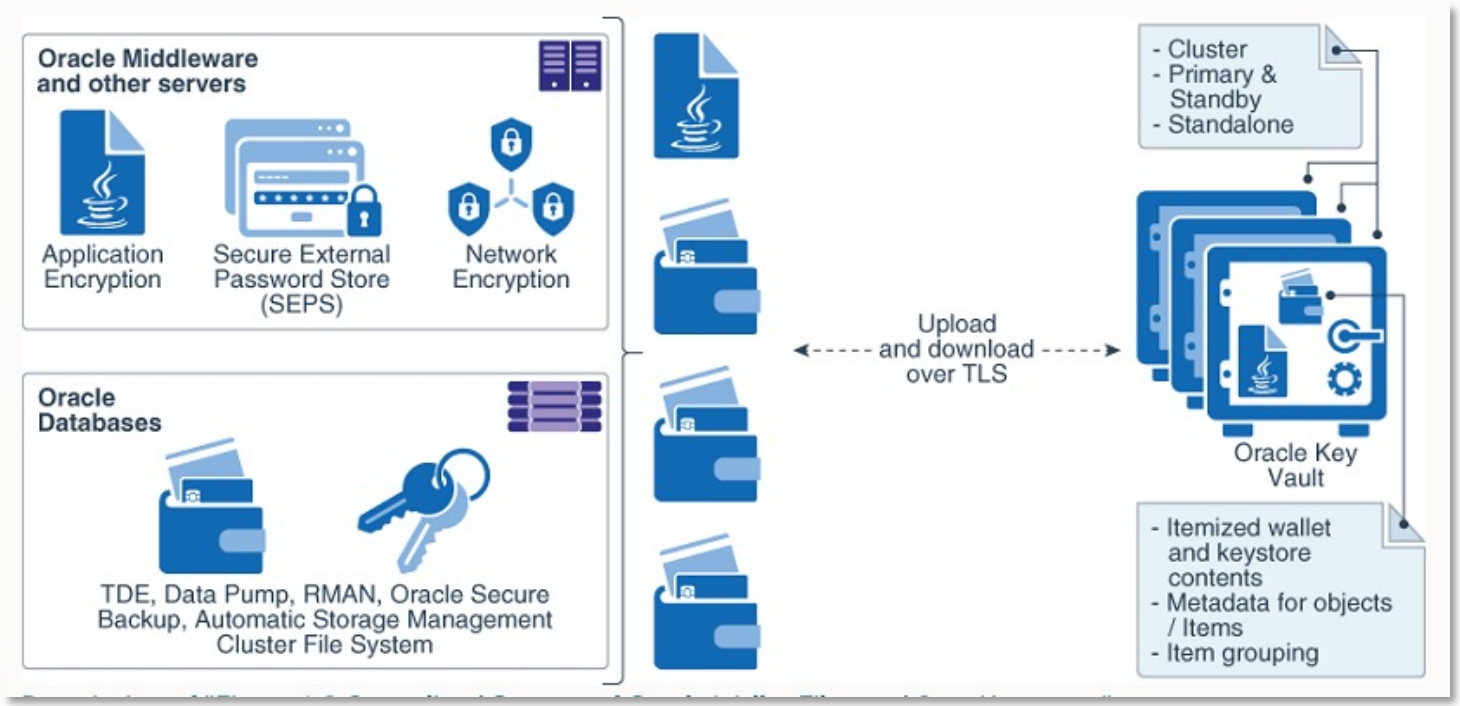
```
#!/bin/bash
set +x
App_name=
KMIP_ID=$(okv managed-object object locate --name $App_name | jq -r '.value.uuids[0]')
password=$(okv managed-object secret get --uuid ${KMIP_ID} | jq -r   '.value.object')
# 把配置文件密码代替换真实的密码
sed -i '/Oracle_Key_Vault_Replace_Password1/$password/g' /u01/app/glassfish/hr_dev_pdb1/WEB-INF/web.xml
sh /u01/app/glassfish/startGlassfish.sh
sleep 1
#真实的密码代替换Oracle_Key_Vault_Replace_Password1
sed -i '/$password/Oracle_Key_Vault_Replace_Password1/g' /u01/app/glassfish/hr_dev_pdb1/WEB-INF/web.xml
~
```

OKV应用场景

OKV应用场景1 – 集中管理Oracle wallet 和 Java keystores

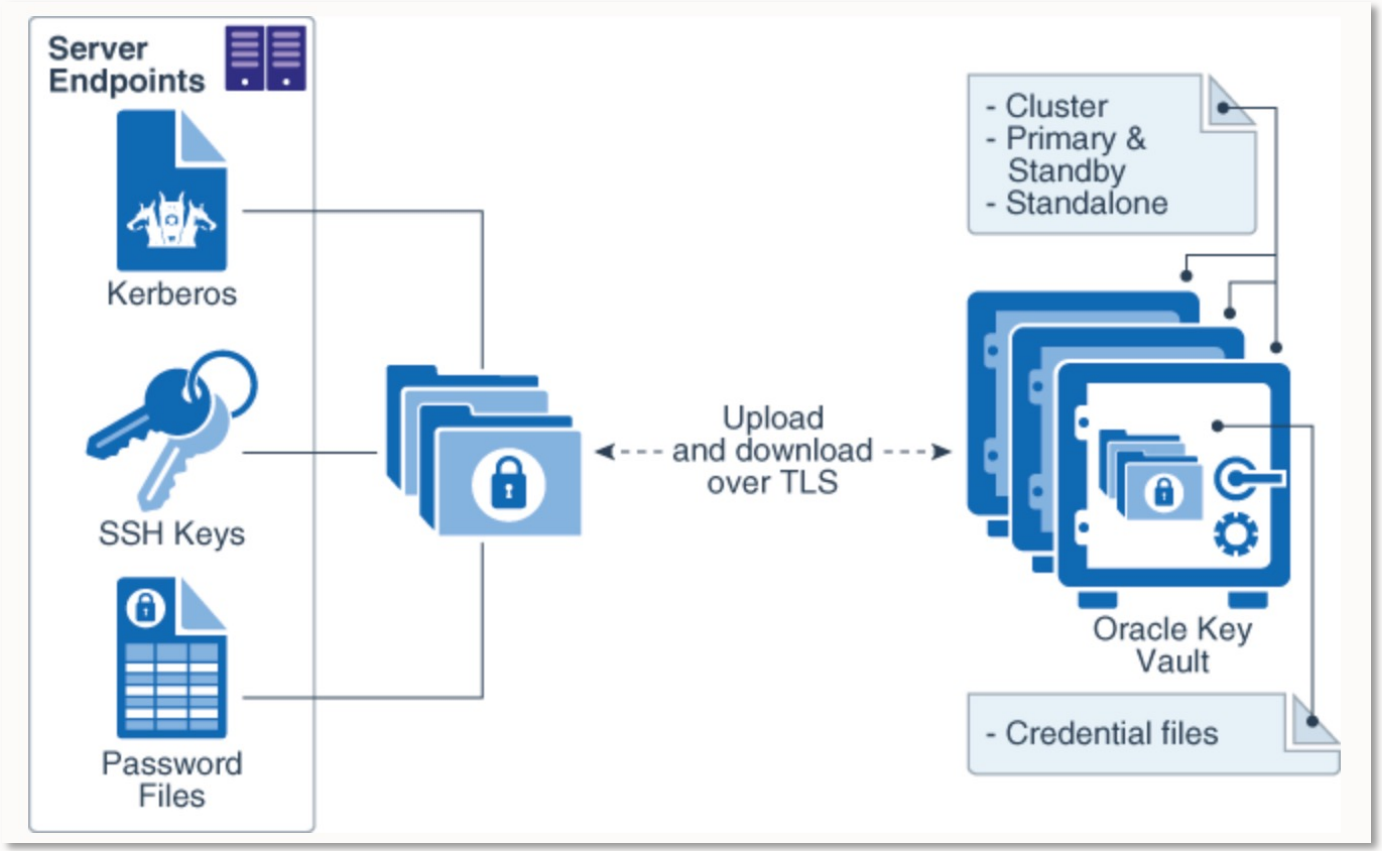
可以将安全对象集中存储在 Oracle Key Vault 中，并使用自动跟踪、备份和恢复机制对其进行管理。

- Oracle Wallet(钱包文件)
  - ✓ 用于加密的对称密钥（包括 TDE 主加密密钥）、密码（安全外部密码存储）和 X.509 证书（网络加密）。
  - ✓ Oracle Key Vault 支持来自所有受支持的 Oracle 数据库版本的钱包文件。
- Java keystore
  - ✓ 对称密钥、非对称密钥（如私钥）和 X.509 证书。
  - ✓ 支持 JKS 和 JCEKS 类型的 Java 密钥库。



OKV应用场景2 – 集中管理凭证文件（密码与秘钥）

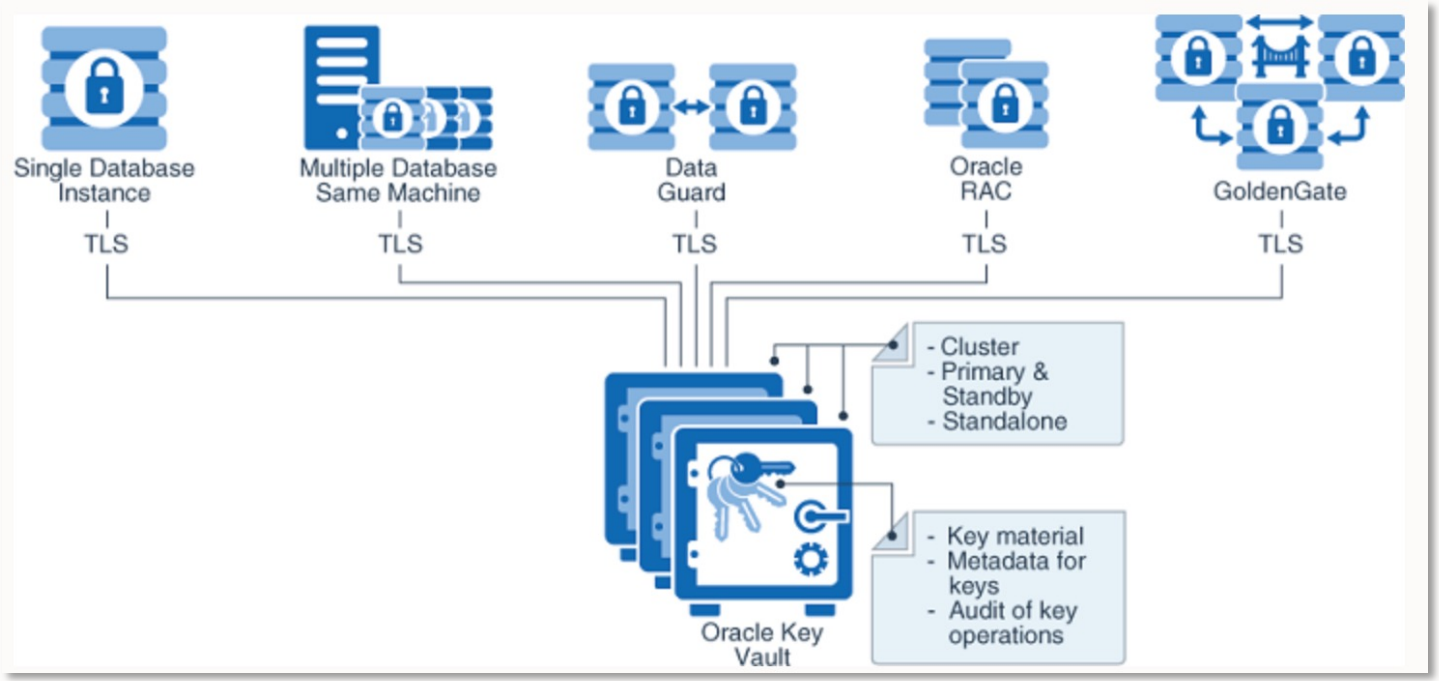
- Oracle Key Vault 可以备份除 Oracle 钱包和 Java 密钥库之外的凭证文件（密码，SSH秘钥等），以便长期保留和恢复。
- Oracle Key Vault 不解析凭证文件里的实际内容。 只是将整个文件存储为不透明对象，以便终端获取该凭证文件。
- 凭证文件包含密钥、密码、SSH 密钥、Kerberos 文件和 X.509 证书。



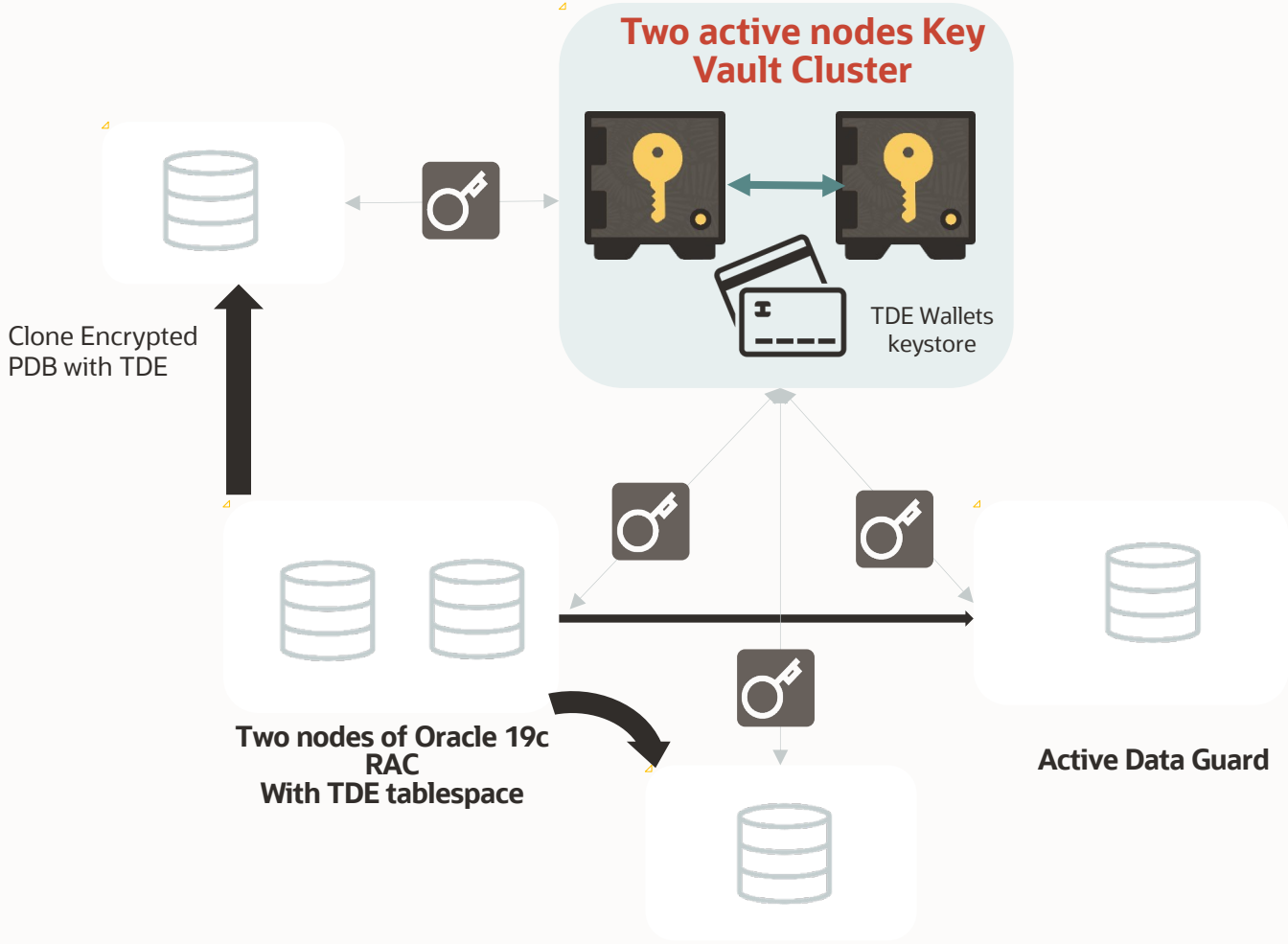
OKV应用场景3 – 集中管理 TDE 主加密密钥

- 在线主密钥能够通过网络连接集中管理透明数据加密 (TDE) 的主密钥，以替代使用本地 Oracle 钱包文件。

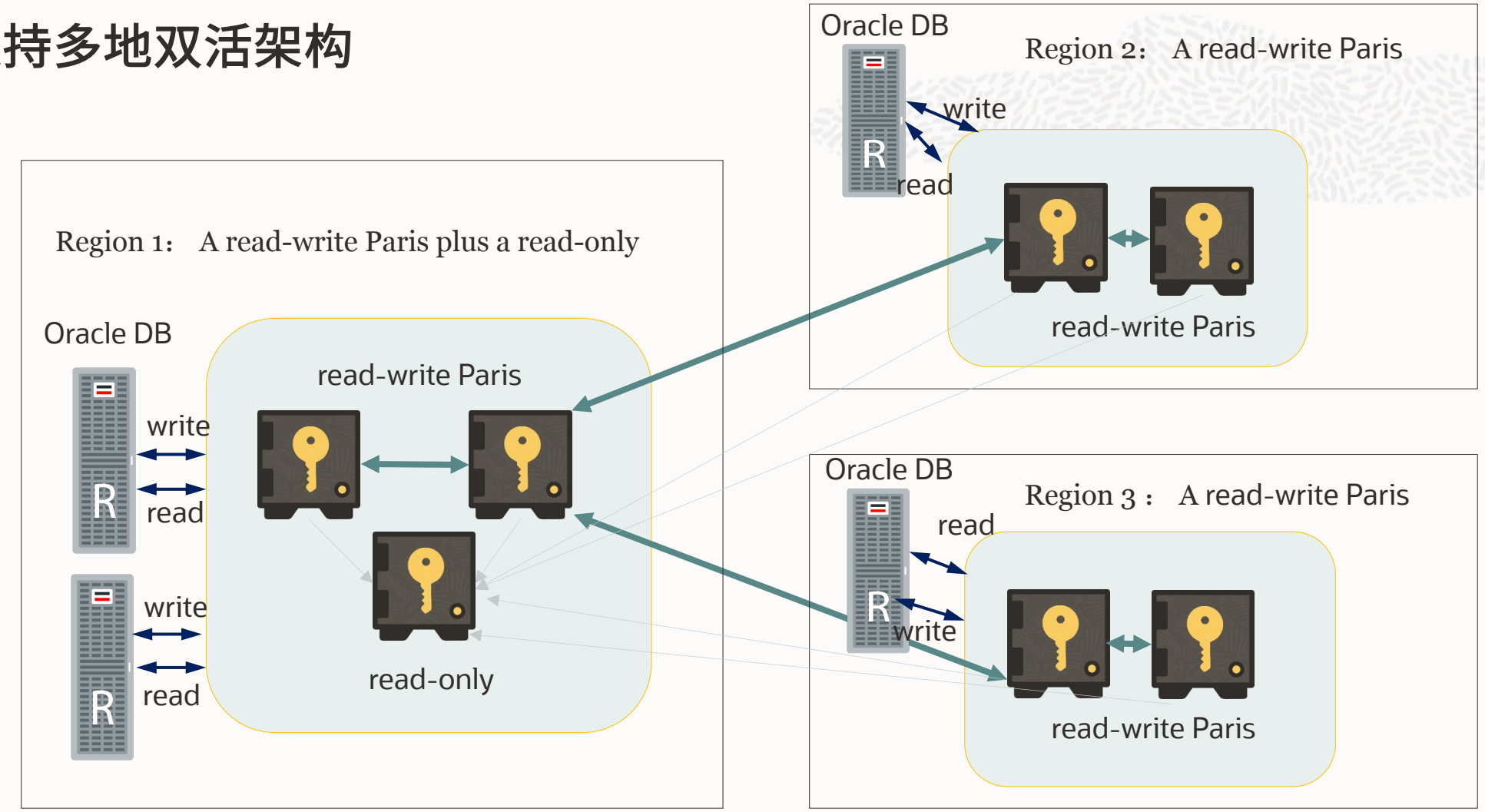
- 在线主密钥也是手动将本地钱包文件复制到多个端点的便捷替代方案。
  - ✓ 比如：当 TDE 在 Oracle Real Application Clusters (Oracle RAC) 或 Oracle Data Guard 等数据库集群上运行时，共享 TDE 主加密密钥而不是维护本地钱包副本



OKV管理TDE key常见架构（RAC+ADG+Restore DB）



OKV支持多地双活架构



Reference:

https://docs.oracle.com/en/database/oracle/key-vault/21.5/okvag/multimaster_concepts.html#GUID-583277E3-5BB4-4D73-8000-C6D6A440C4DB

客户案例-某政府某职能部门

客户需求：

客户大量使用TDE数据库加密功能以及脚本密码，需要集中式密钥管理系统来管理TDE的密钥以及用户密码和密钥，密钥管理系统还必须高度可用且安全。

客户的选择：

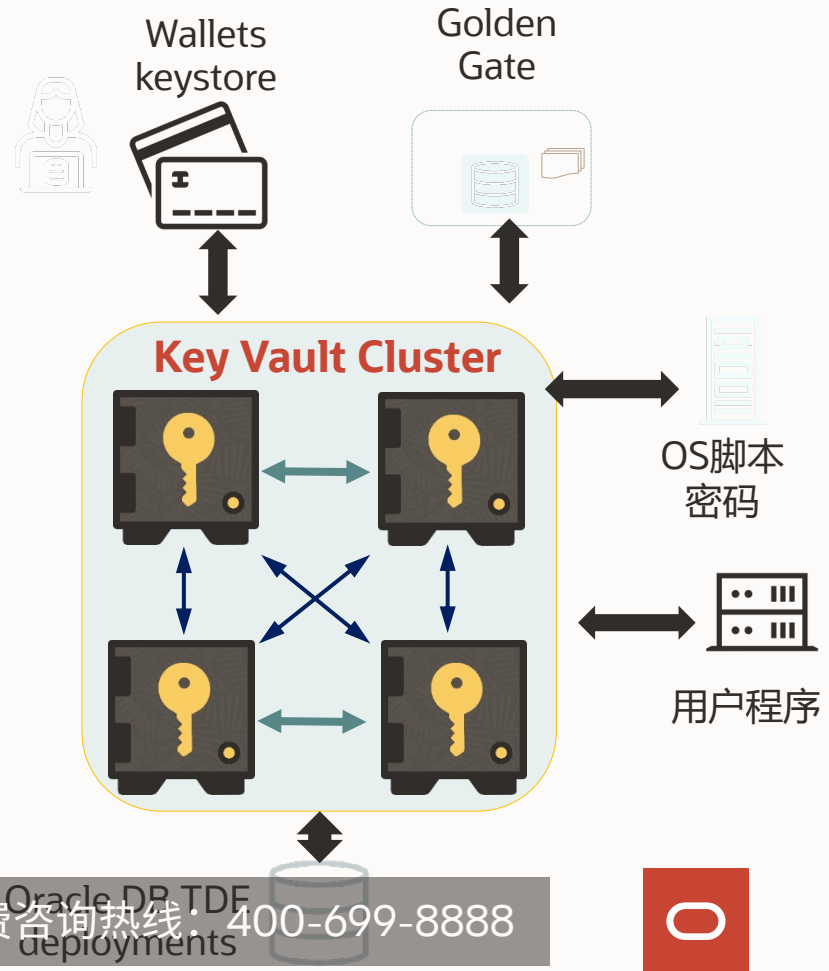
客户购买了 14 台 Oracle Key Vault (OKV) 并快速迁移其 TDE 密钥以利用 OKV 的快速性能、高可用性和可扩展性，他们重新调整了硬件安全模块的用途以与 OKV 集成，充当信任以满足安全要求。

为什么选择 Oracle Key Vault (OKV)：

- OKV 为 Oracle 数据库工作负载提供更佳性能。
- 多主集群架构提供密钥的持续可用性。
- OKV 读/写对架构提供密钥的持续可用性。
- 相同的 OKV 可用于管理TDE以及Oracle GoldenGate密钥，以降低复杂性并增强安全性
- 可以管理脚本密码及程序配置敏感信息。

这对客户意味着什么：

1. 支持高性能、高可用性和安全的密钥管理系统。
2. Oracle Key Vault 提供的集中式密钥管理在针对安全事件和勒索软件的公司战略中发挥着重要作用。
3. 客户可以快速将新节点添加到他们的 OKV 网络，无论它们部署在哪里。
4. 客户可以利用 OKV 灵活的集群机制来帮助满足监管要求，包括数据驻留限制。



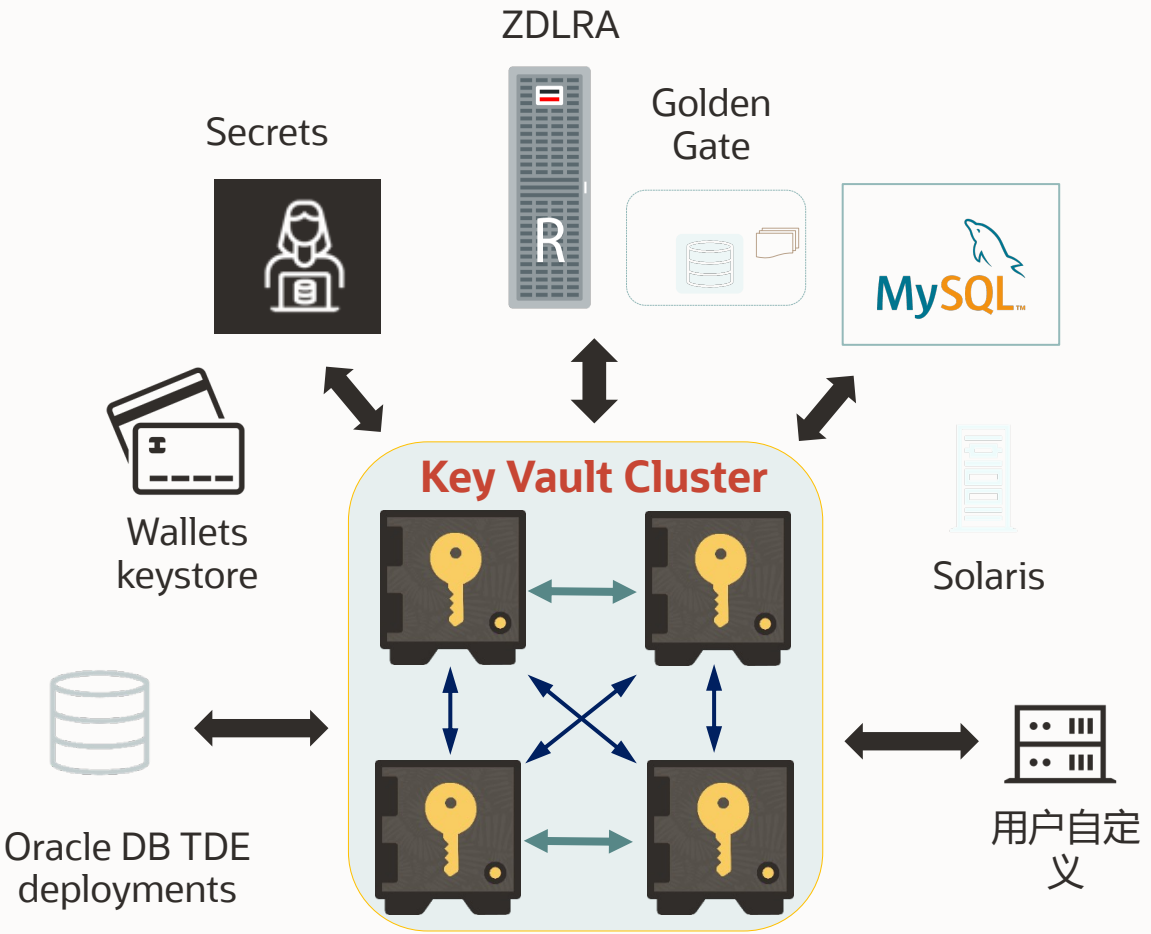
OKV动手演示

DEMO演示

1: OKV界面以及概念的介绍

2: OKV管理TDE Master key

3: OKV管理数据库密码



Q/A

Oracle GoldenGate微服务架构的实现及案例分享

数据库和云系列讲座

胡鑫

- CSS 资深架构师
- 17年+数据库解决方案和运维管理经验
- 14年+Goldengate架构设计、运维管理经验

内容简介

- OGG 微服务简介
- OGG 微服务架构实施案例
- 基于OGG 微服务restful API使用案例

Zoom直播

直播时间：9月15日 11:00 - 12:00
扫描二维码进入直播
Zoom ID：957 9669 6723
密码：20212023

微信扫一扫预约

数据库和云讲座群

20-21

甲骨文云技术公众号

技术专家1V1深入交流