Encrypt Your Crown Jewels and Manage Keys Efficiently with Oracle Key Vault

TRN4106 – October 24, 2018

Michael Mesaros
Director, Database Security Product Management
Oracle Database Security

Hamid Habet
IT Infrastructure Shared Services
Allianz Technology SE

Rahil Mir
Software Development Manager
Oracle Database Security

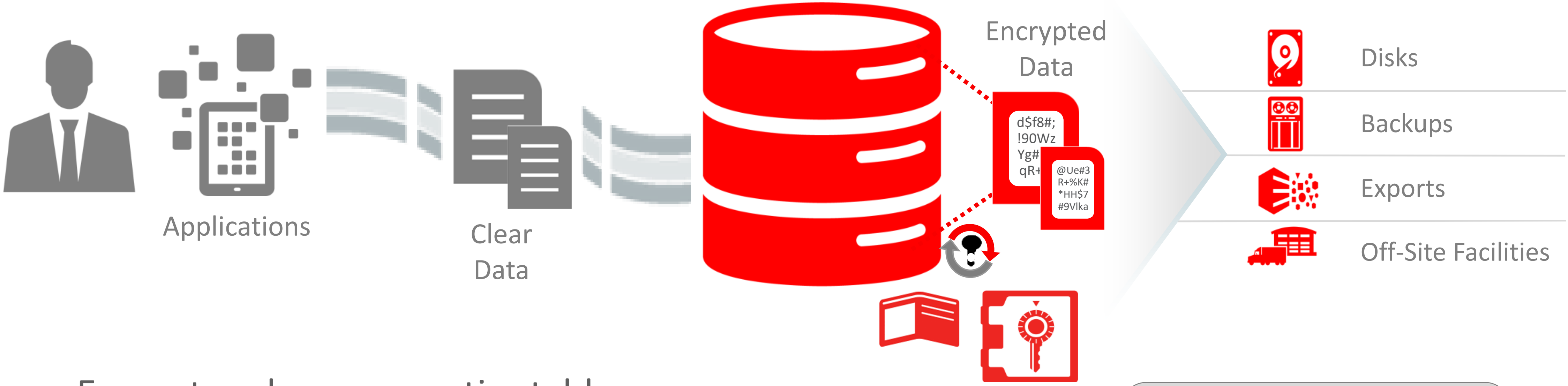
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Program Agenda

1. Oracle Transparent Data Encryption (TDE)
2. Overview of Oracle Key Vault
3. Oracle Key Vault Directions
4. Oracle Key Vault Customer Use Case

Oracle Transparent Data Encryption (TDE)



- Encrypts columns or entire tablespaces
- Protects the database files on disk and in backups
- High-speed performance
- Transparent to applications, no changes required
- Integrated with Oracle technologies

Oracle TDE Innovations

Future

Oracle Database 18c

- Bring Your Own TDE Master Encryption Key (BYOK) into the database
  - Supports AES256, ARIA256, SEED128, GOST256
- Per-PDB wallets
  - Each PDB can manage its own keystore
- Easier data migration to the cloud
  - RMAN backup/restore clear or encrypted on-premises data to the cloud (automatically encrypted)
- FIPS 140-2 Level 1 Cryptographic Module
  - Approved encryption suites for SSL/TLS and TDE

Oracle Database 19c

- Oracle Managed Tablespace Encryption
  - TDE now encrypts Oracle Data Dictionary
- FIPS update
  - Encryption tools (orapki, mkstore) updated with FIPS compliant libraries

ORACLE

TDE Tablespace Conversion

Customer need

- Regulations such as EU-GDPR making encryption an imperative
- Typical customers may have 100+ TBs of data requiring conversion
- Has to be accomplished with
  - Limited storage/compute resources
  - Limited staff
  - Little/no downtime windows

Conversion Options

- Online tablespace encryption
  - Encrypts tablespace in background with no downtime
  - Storage overhead is 2x the largest tablespace file
  - Available on Oracle 12c Release 2
- Fast offline tablespace conversion
  - Simultaneous encryption of multiple data files across multiple cores
  - No storage overhead
  - Also available for 12.1.0.2 and 11.2.0.4

ORACLE

TDE Tablespace Conversion Customer Experience

Customer situation

- Three databases with a total size of 140 TB
    - About 500 datafiles to encrypt
- Limitations
    - Limited extra storage available
    - Limited downtime window
    - Complex application environments
- Existing DataGuard environment

Result

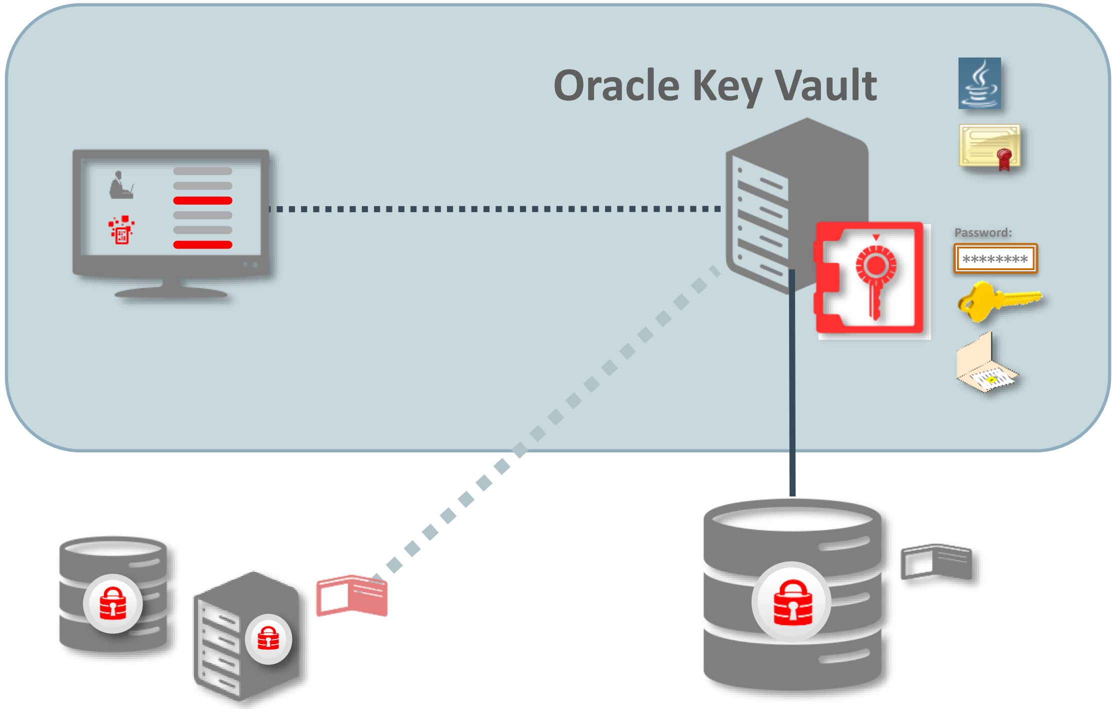
- Selected fast offline conversion with DataGuard
    - Minimal downtime
    - Simple solution
    - Least impact to production system
- Strategies
    - Ran multiple encryption threads in parallel
    - Grouped datafiles threads based on similar sizing

Program Agenda

1. Oracle Transparent Data Encryption (TDE)
2. Overview of Oracle Key Vault
3. Oracle Key Vault Directions
4. Oracle Key Vault Customer Use Case

ORACLE

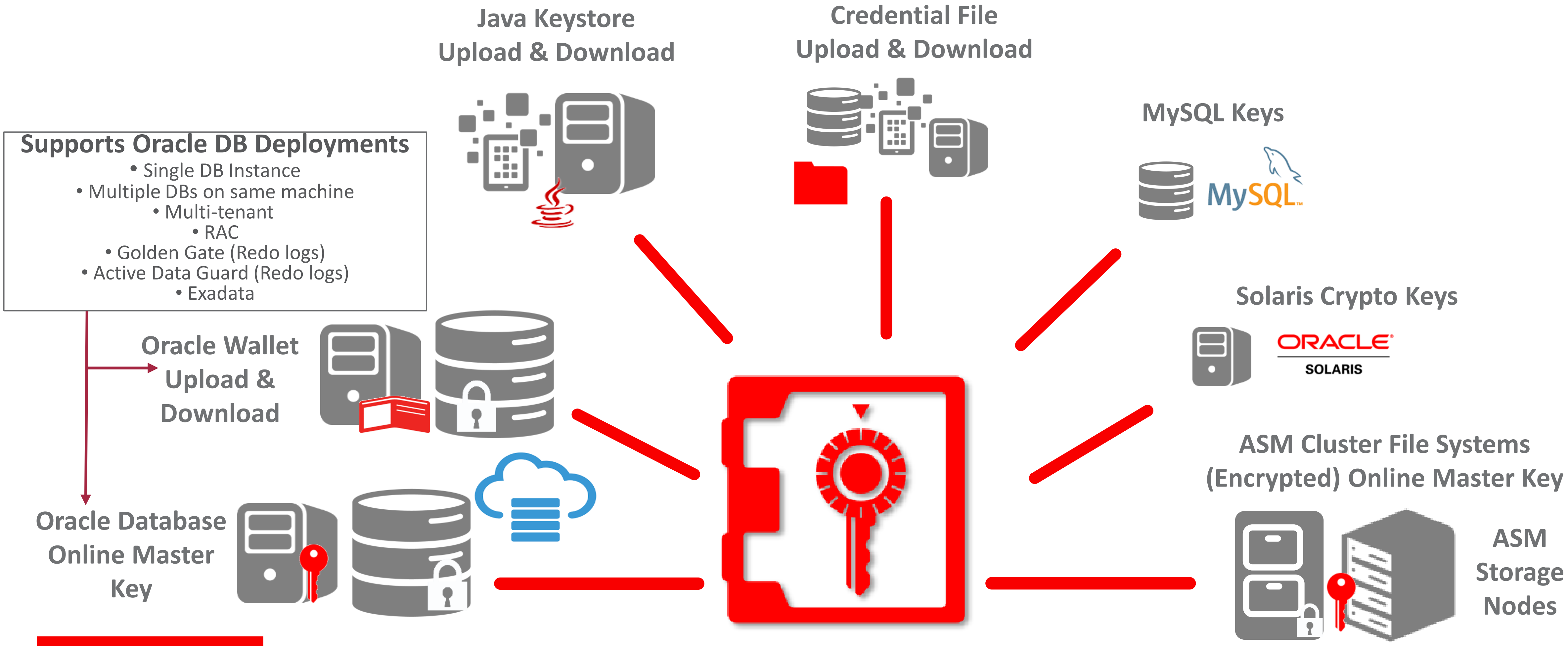
Oracle Key Vault: Store and Manage Encryption Keys



Oracle Wallet, MySQL, Java Keystores, ACFS, Solaris Crypto keys, Kerberos, ssh, …

- Optimized for TDE master key management for 100s of databases
- Prevents Key Loss due to forgotten password or accidental deletion of wallets and Java keystores
- Supports popular hardware security modules as root of trust
- Robust, secure, and standards compliant (OASIS KMIP)
- Field-proven technology stack

Oracle Key Vault Use Cases



Supports Oracle DB Deployments

- Single DB Instance
- Multiple DBs on same machine
- Multi-tenant
- RAC
- Golden Gate (Redo logs)
- Active Data Guard (Redo logs)
- Exadata

Java Keystore Upload & Download
Credential File Upload & Download
MySQL Keys
MySQL
Solaris Crypto Keys
ORACLE
SOLARIS
ASM Cluster File Systems (Encrypted) Online Master Key
ASM Storage Nodes
Oracle Wallet Upload & Download
Oracle Database Online Master Key

Recent Oracle Key Vault 12.2 Feature Innovations

- Improved availability
  - Read-only restricted mode
  - Persistent master key cache support
  - Quick discovery of unreachable OKV Servers
- Improved manageability
  - Endpoint configuration is now centralized in the OKV server and pushed to the endpoints
  - Remote syslog support for audit records
- Improved support
  - Support for UEFI boot (Oracle Server X7-2)
  - Expanded AIX (5.3) and Windows endpoint support

Program Agenda

1. Oracle Transparent Data Encryption (TDE)
2. Overview of Oracle Key Vault
3. Oracle Key Vault Directions
4. Oracle Key Vault Customer Use Case

ORACLE®

Goals for the Next Oracle Key Vault Release

- New enterprise features, with improved:
  - High availability
  - Disaster recovery
  - Load distribution
  - Geographic distribution
- Broaden support for custom applications
- Expand FIPS validation footprint
- Update platform to the latest Oracle infrastructure

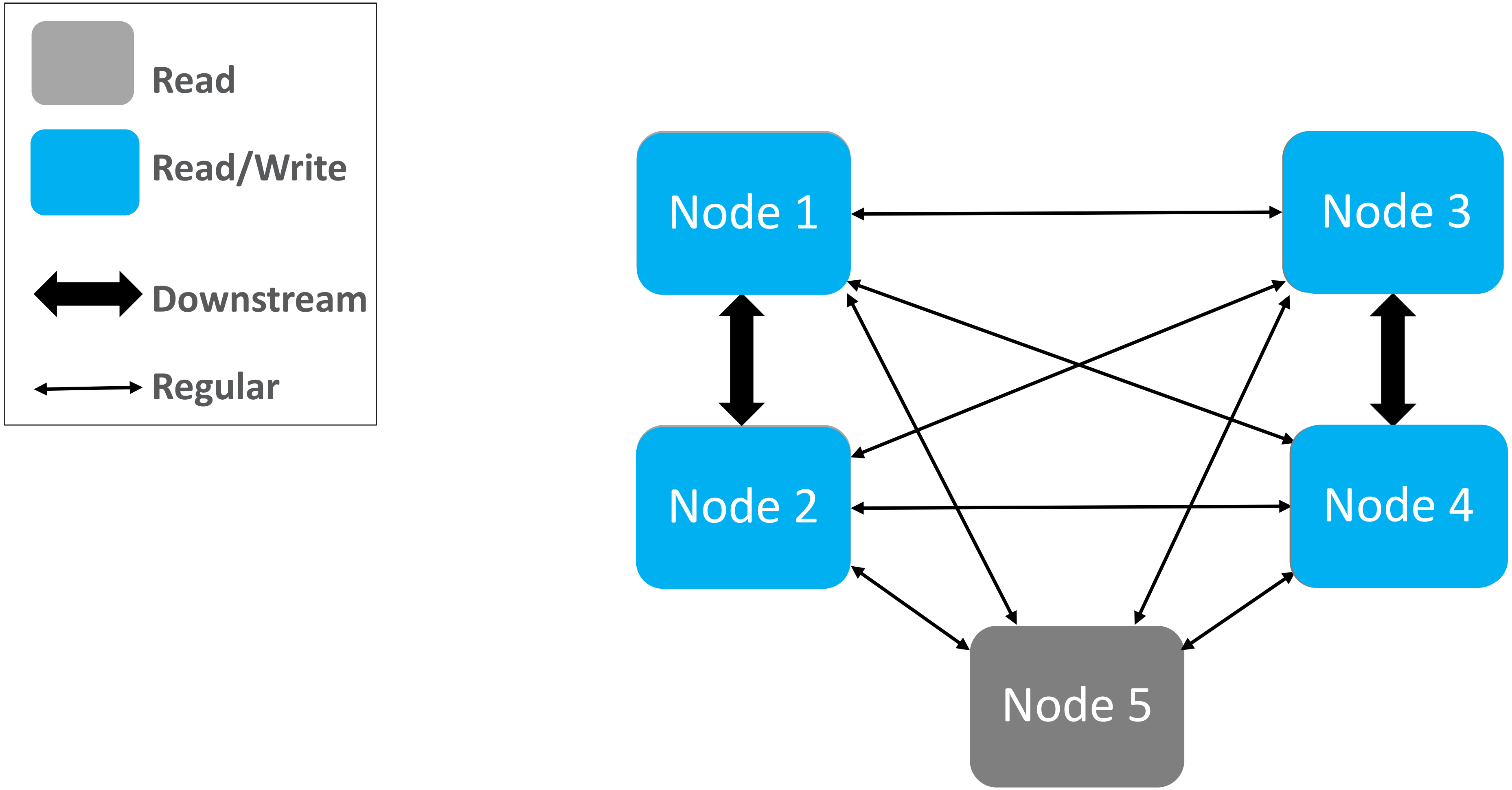
ORACLE

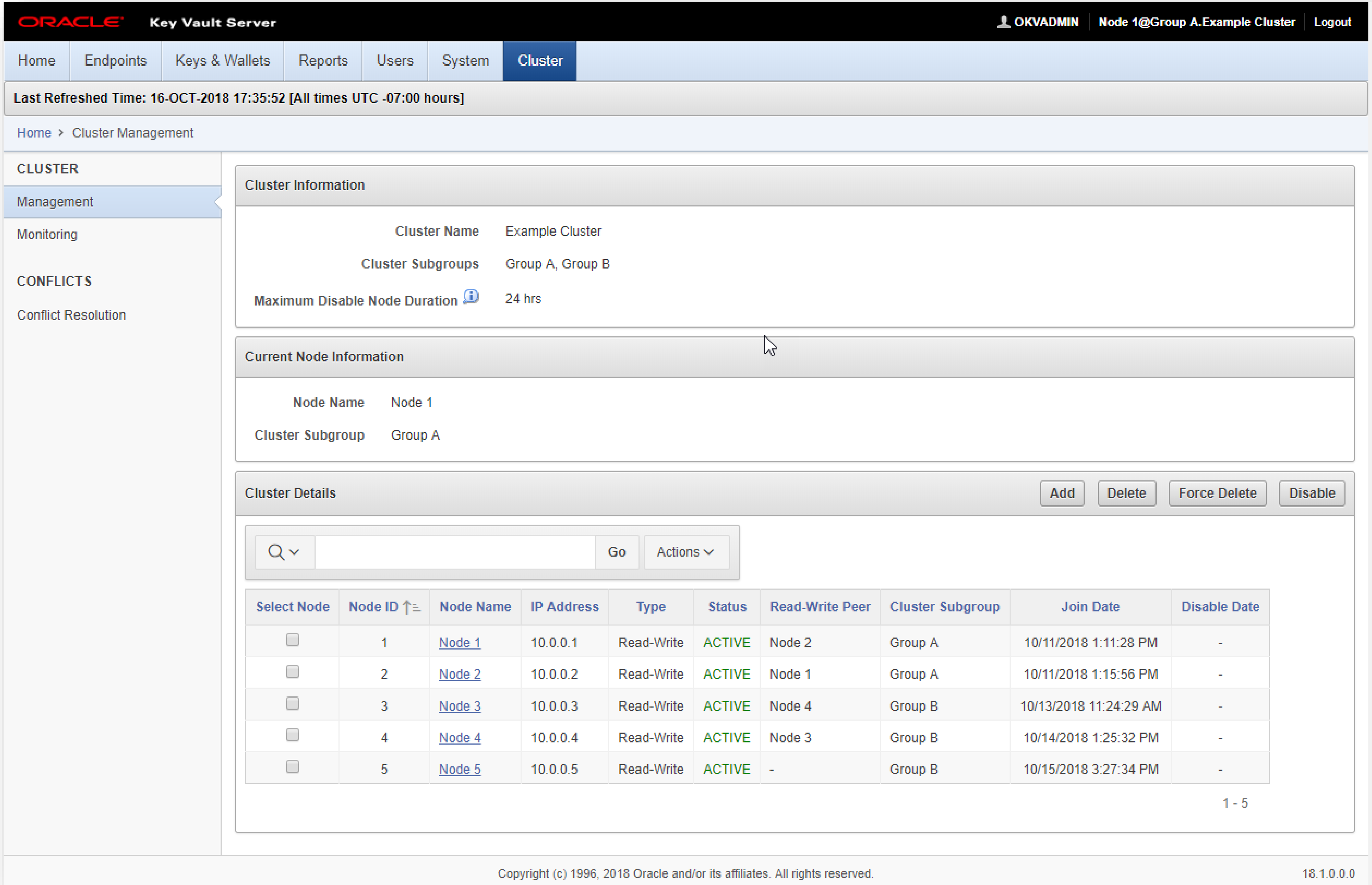
Future

Upcoming OKV Multi-Master Cluster Functionality

- Read-Write node pairs
  - Pairs of nodes with bi-directional synchronous replication between them
  - Both nodes are active and can respond to read-write requests
- OKV nodes deployed in a cluster
  - Each node communicates with all other nodes
  - Minimal information lag between nodes
  - Support for large geographically distributed deployments
- Optional read-only nodes
  - Asynchronously replicate with read-write nodes
  - Improved load balancing, availability
- Endpoint scan lists
  - Every node is available to every endpoint
  - Scan lists created and maintained automatically
  - Near zero downtime for endpoints during applying patches and upgrades

OKV Cluster Deployment Example





Last Refreshed Time: 16-OCT-2018 17:35:52 [All times UTC -07:00 hours]

Cluster Information

Cluster Name	Example Cluster
Cluster Subgroups	Group A, Group B
Maximum Disable Node Duration	24 hrs

Current Node Information

Node Name	Node 1
Cluster Subgroup	Group A

Cluster Details

Select Node	Node ID	Node Name	IP Address	Type	Status	Read-Write Peer	Cluster Subgroup	Join Date	Disable Date
☐	1	Node 1	10.0.0.1	Read-Write	ACTIVE	Node 2	Group A	10/11/2018 1:11:28 PM	-
☐	2	Node 2	10.0.0.2	Read-Write	ACTIVE	Node 1	Group A	10/11/2018 1:15:56 PM	-
☐	3	Node 3	10.0.0.3	Read-Write	ACTIVE	Node 4	Group B	10/13/2018 11:24:29 AM	-
☐	4	Node 4	10.0.0.4	Read-Write	ACTIVE	Node 3	Group B	10/14/2018 1:25:32 PM	-
☐	5	Node 5	10.0.0.5	Read-Write	ACTIVE	-	Group B	10/15/2018 3:27:34 PM	-

1 - 5

18.1.0.0.0

Future

More Upcoming Oracle Key Vault Features

- REST-ful interface for Key Management
  - In addition to existing REST support for endpoint enrollment and provisioning
  - Extensibility and ability to integrate with custom apps
- C and Java Client SDK
  - Extensibility and ability to integrate with custom applications, more mileage from same OKV infrastructure
- “FIPS-Inside”
  - FIPS validated Crypto Module (RSA BSAFE) for core functions of key creation and storage
  - FIPS validated OpenSSL Crypto Module on Oracle Linux for remote administration and service management
- Upgrade of the embedded database to latest Oracle Database 18c release

ORACLE

Program Agenda

1 Oracle Transparent Data Encryption (TDE)

2 Overview of Oracle Key Vault

3 Oracle Key Vault Directions

4 Oracle Key Vault Customer Use Case

ORACLE

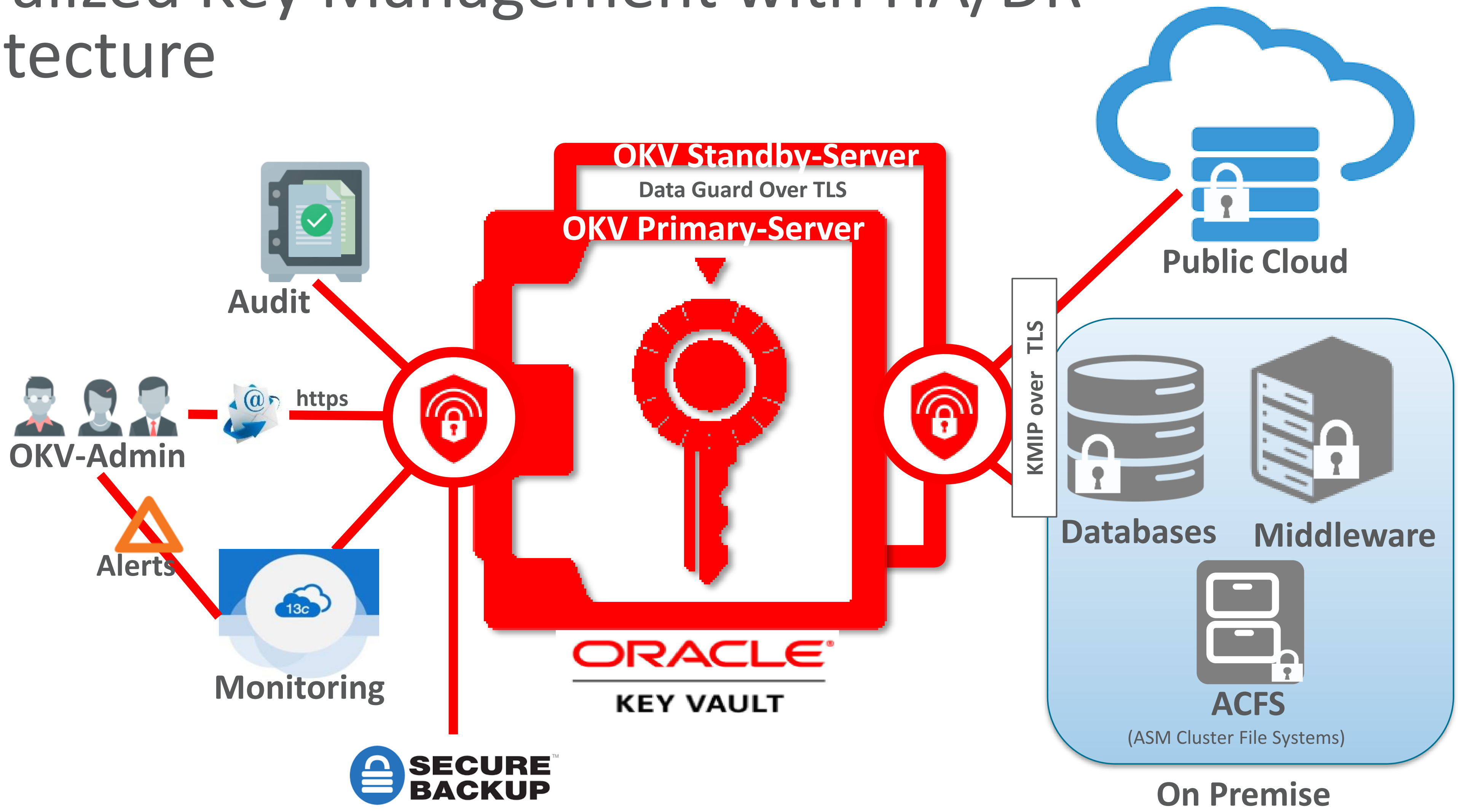
Business Drivers for Centralized Key Management

- Fulfill EU-GDPR requirements
  - Encryption and Key Mgmt. (Article 32: Pseudonymisation and Encryption of Personal Data)
- Centralized Key store
  - Stream line operational complexity of managing software wallets across a large enterprise environment
- Key Availability
  - Prevent Key Loss due to forgotten password, accidental deletion or stolen credential
- Public Cloud
  - On-Premise Key Management for encrypted Systems offered in Public Cloud

- Separation of Duties
  - Enforce Separation between Keys and Data Management
- Automation
  - Using RESTfull-API for Endpoint Management
- Maximum Security Architecture
  - Shrink the attack surface and reduce the number of ways in which attackers can access the data
  - Long-term Retention
  - Simplify Operations
  - Full auditing and Alerts

Allianz

Centralized Key Management with HA/DR Architecture



ORACLE

Separation of Duties

- OKV-Admin activities with no access to DB-Servers
  - OKV-Setup with HA/DR Architecture
  - Backup & Recovery
    - Remote Backup on ACFS
  - Monitoring via Cloud Control
    - KMIP and HTTP Daemons
    - Database
    - File System (e.g.: /var/lib/oracle)
  - Delivery of Restfull-API scripts incl. okvrestservices.jar (required for EP-Provisioning)
  - OKV-Patching and delivery of actual software library after patching
    - okvrestservices.jar (Required for new EP provisioning with actual version)
    - okvclient.jar (required to update already existing EP library to the actual version)
  - Download PWD from OKV using Unique Identifier
  - Reporting

- DBA activities without access to OKV-GUI and OKV-Servers
  - EP-Management
    - EP-Provisioning using Restfull-API
    - EP-Installation using defined naming convention
    - Encryption Data-at-Rest using TDE and OKV as Key Management System
    - Upload PWD into OKV
    - Access Mgmt. for daily-operations tasks (e.g.: Exp/Imp, DB-Cloning)
      - Grant read access to EP
      - Re-Key
      - Revoke read access from EP
    - Delete EP after DB-Decommission
  - Activities to be executed after OKV-Patching
    - Install actual Software Library okvclient.jar (required to update each existing EP library to the actual version)

Encryption Data-at-Rest and Key Management

Separation of Duties

OKV-Admin

1 OKV-Setup, Backup&Recovery and Monitoring

2 Delivery of:
```
- Restfull-API scripts
- okvrestservices.jar
```

DBA- Activities per EP

3 Endpoint Provisioning

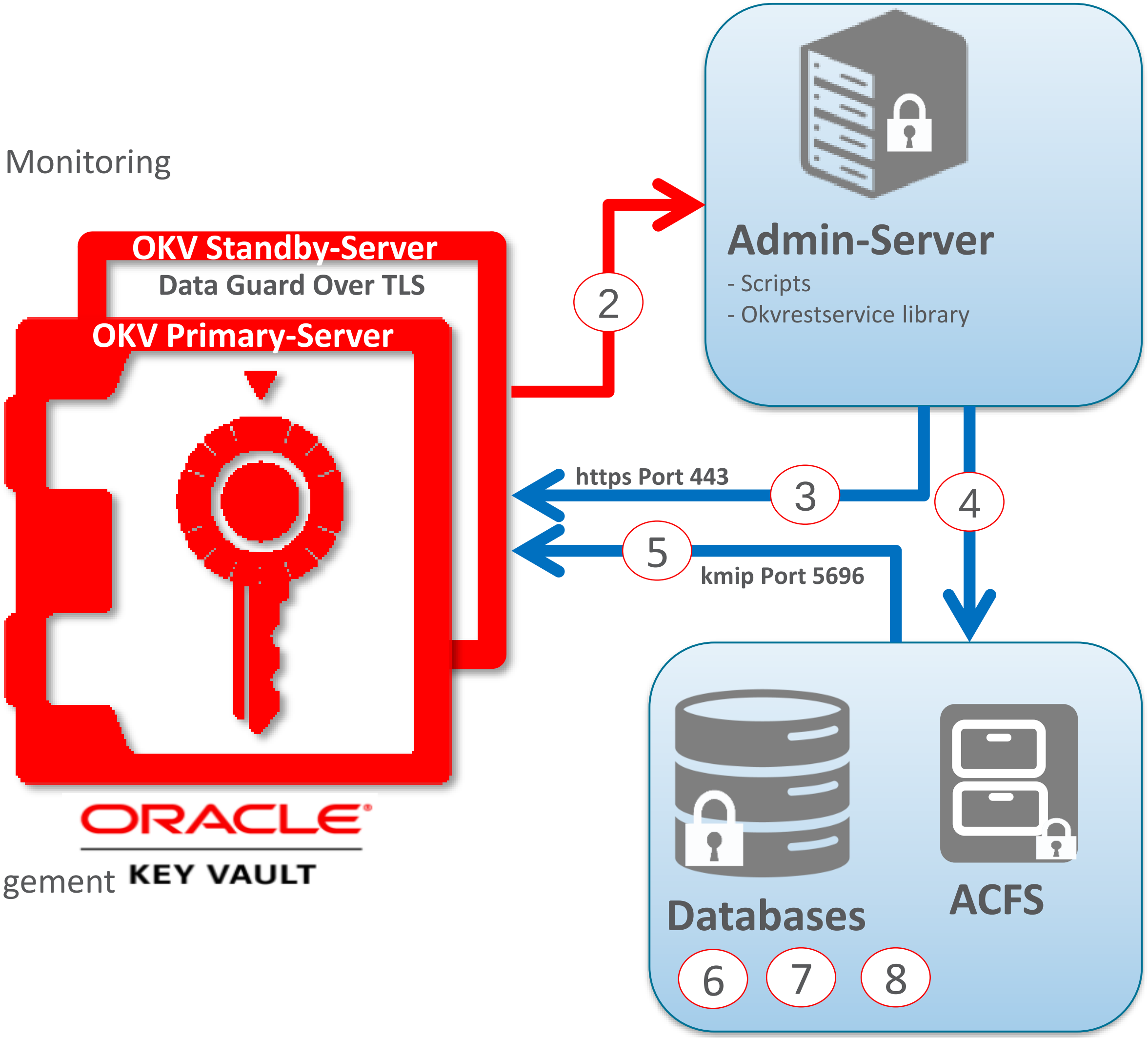
4 Copy generated okvclient jar file

5 Install okvclient jar file

6 root.sh per Host once

7 Encryption using OKV for Key Management

8 Upload PWD into OKV



OKV Standby-Server

Data Guard Over TLS

OKV Primary-Server

ORACLE KEY VAULT

2

Admin-Server

- Scripts
- Okvrestservice library

https Port 443

3

4

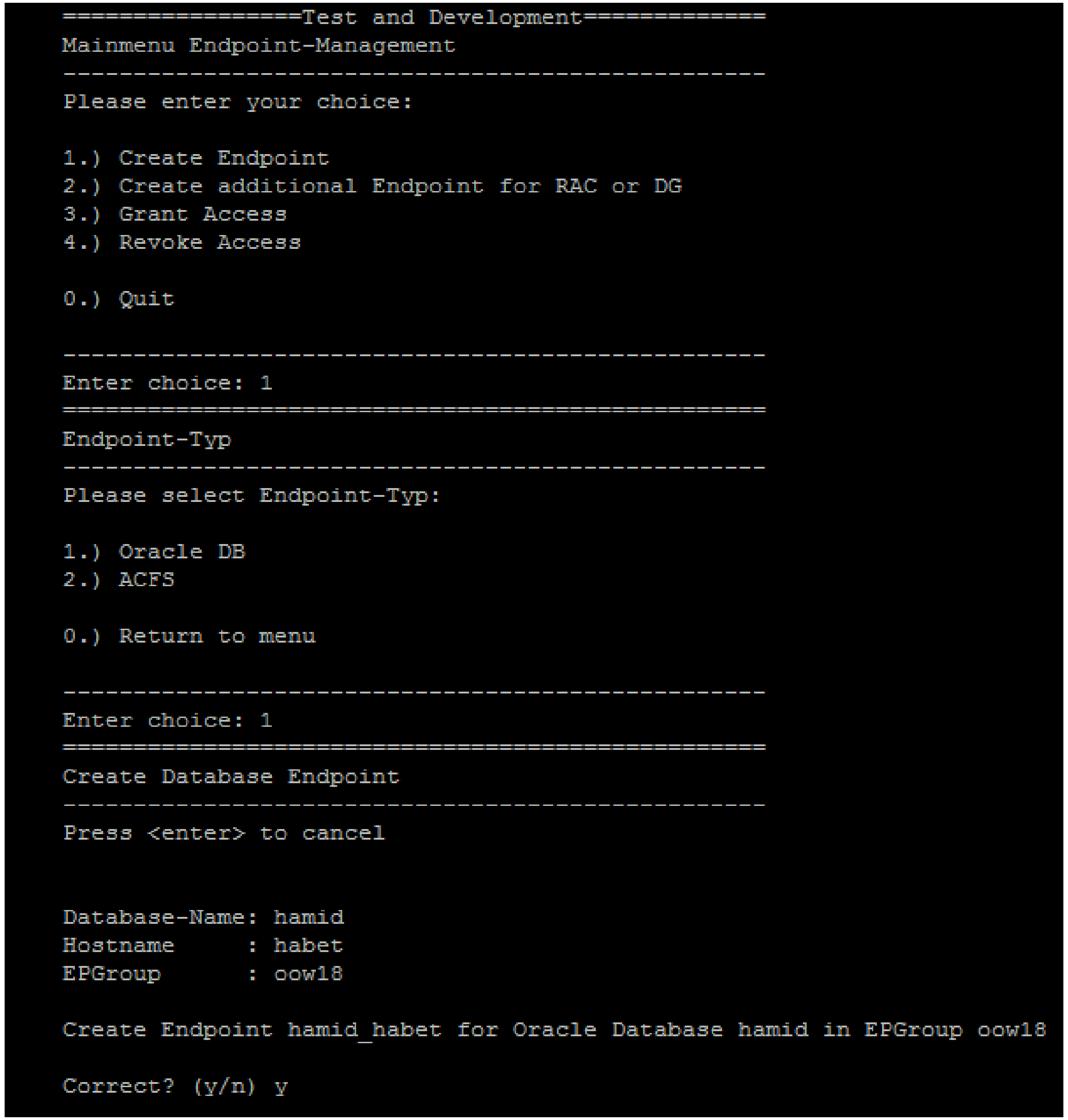
5

kmip Port 5696

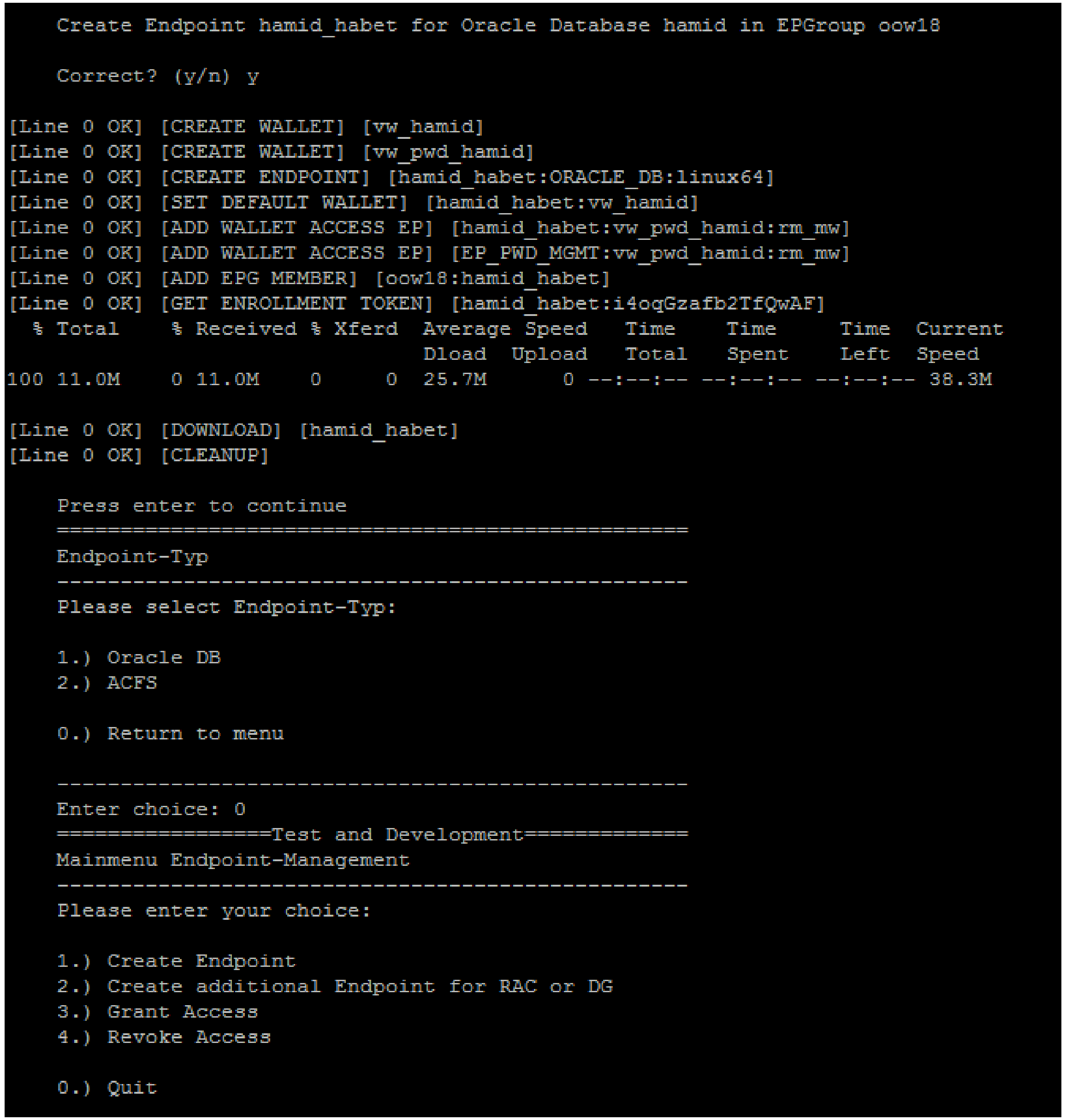
Databases

ACFS

6 7 8



```
=================Test and Development=============
Mainmenu Endpoint-Management
--------------------------------------------------
Please enter your choice:

1.) Create Endpoint
2.) Create additional Endpoint for RAC or DG
3.) Grant Access
4.) Revoke Access

0.) Quit

--------------------------------------------------
Enter choice: 1
==================================================
Endpoint-Typ
--------------------------------------------------
Please select Endpoint-Typ:

1.) Oracle DB
2.) ACFS

0.) Return to menu

--------------------------------------------------
Enter choice: 1
==================================================
Create Database Endpoint
--------------------------------------------------
Press <enter> to cancel


Database-Name: hamid
Hostname     : habet
EPGroup      : oow18

Create Endpoint hamid_habet for Oracle Database hamid in EPGroup oow18

Correct? (y/n)  y
```



```
    Create Endpoint hamid_habet for Oracle Database hamid in EPGroup oow18

    Correct? (y/n)  y

[Line 0 OK] [CREATE WALLET] [vw_hamid]
[Line 0 OK] [CREATE WALLET] [vw_pwd_hamid]
[Line 0 OK] [CREATE ENDPOINT] [hamid_habet:ORACLE_DB:linux64]
[Line 0 OK] [SET DEFAULT WALLET] [hamid_habet:vw_hamid]
[Line 0 OK] [ADD WALLET ACCESS EP] [hamid_habet:vw_pwd_hamid:rm_mw]
[Line 0 OK] [ADD WALLET ACCESS EP] [EP_PWD_MGMT:vw_pwd_hamid:rm_mw]
[Line 0 OK] [ADD EPG MEMBER] [oow18:hamid_habet]
[Line 0 OK] [GET ENROLLMENT TOKEN] [hamid_habet:i4oqGzafb2TfQwAF]
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11.0M    0 11.0M    0     0  25.7M      0 --:--:-- --:--:-- --:--:-- 38.3M

[Line 0 OK] [DOWNLOAD] [hamid_habet]
[Line 0 OK] [CLEANUP]

    Press enter to continue
    ==================================================
    Endpoint-Typ
    --------------------------------------------------
    Please select Endpoint-Typ:

    1.) Oracle DB
    2.) ACFS

    0.) Return to menu

    --------------------------------------------------
    Enter choice: 0
    =================Test and Development=============
    Mainmenu Endpoint-Management
    --------------------------------------------------
    Please enter your choice:

    1.) Create Endpoint
    2.) Create additional Endpoint for RAC or DG
    3.) Grant Access
    4.) Revoke Access

    0.) Quit
```

Encryption Data-at-Rest and Key Management

Activities after OKV-Patching

Allianz

OKM-Admin Activities

1 OKV-Patch

2 Delivery of actual software libraries:

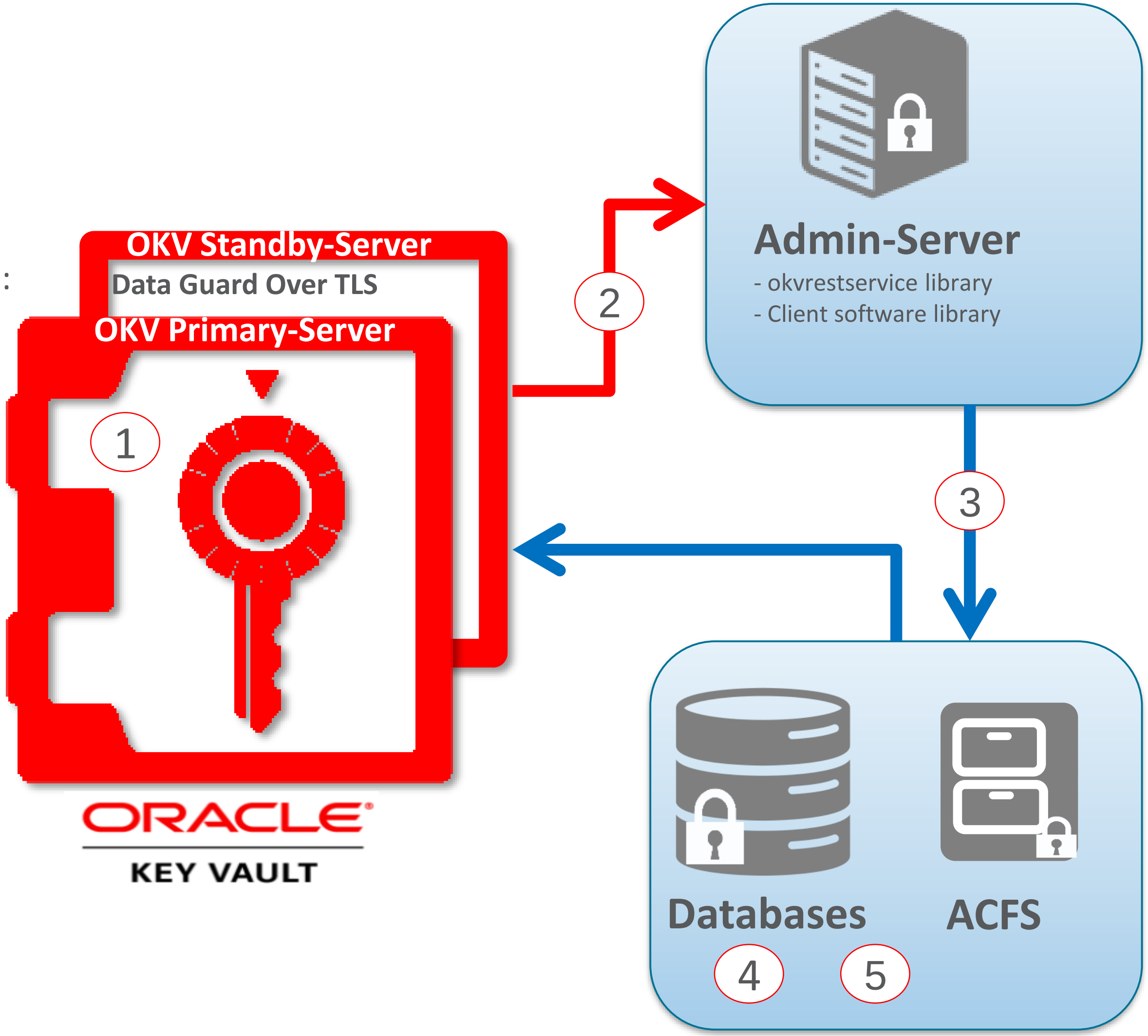
```
–  okvrestservices.jar
–  Okvclient.jar
```

DBA-Activities

3 Copy of new Software Library

4 Install okvclient jar file

5 Execution of root.sh



ORACLE

Customer Experience Summary

- Databases Continue to be the Treasure Hunt for Attackers

  Databases continue to be the most attractive targets for Attackers because they are the information store with all the sensitive data.

  To shrink the attack surface and reduce the number of ways in which attackers can access the databases, it is important to enforce separation of Keys & Master Keys from encrypted Data.

- Oracle Key Vault is the preferred Key Management Tool to enforce separation of duties, shrink attack and simplify daily operations with ACFS and Oracle Database encryption

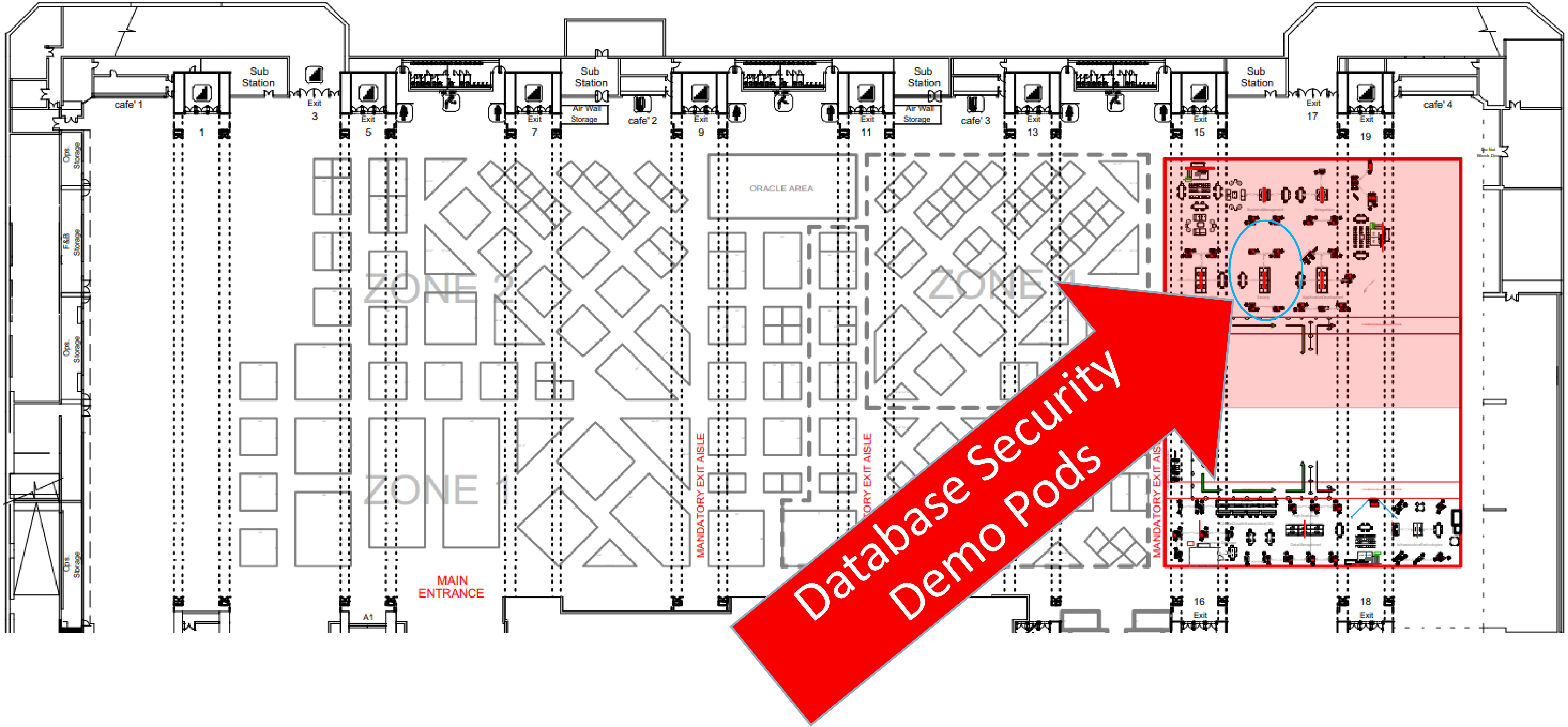
Q & A

Data Security Cloud Service

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Moscone South



Database Security Demo Pods

ORACLE®