Titkosítás tapasztalatai Oracle Cloud alapú Exadata környezetben

By Zsolt Szalóki

Allianz

Agenda

- Oracle Transparent Data Encryption
- Oracle EXADATA Cloud Service (EXACS)
- Oracle Key Vault

Oracle Transparent Data Encryption (TDE)

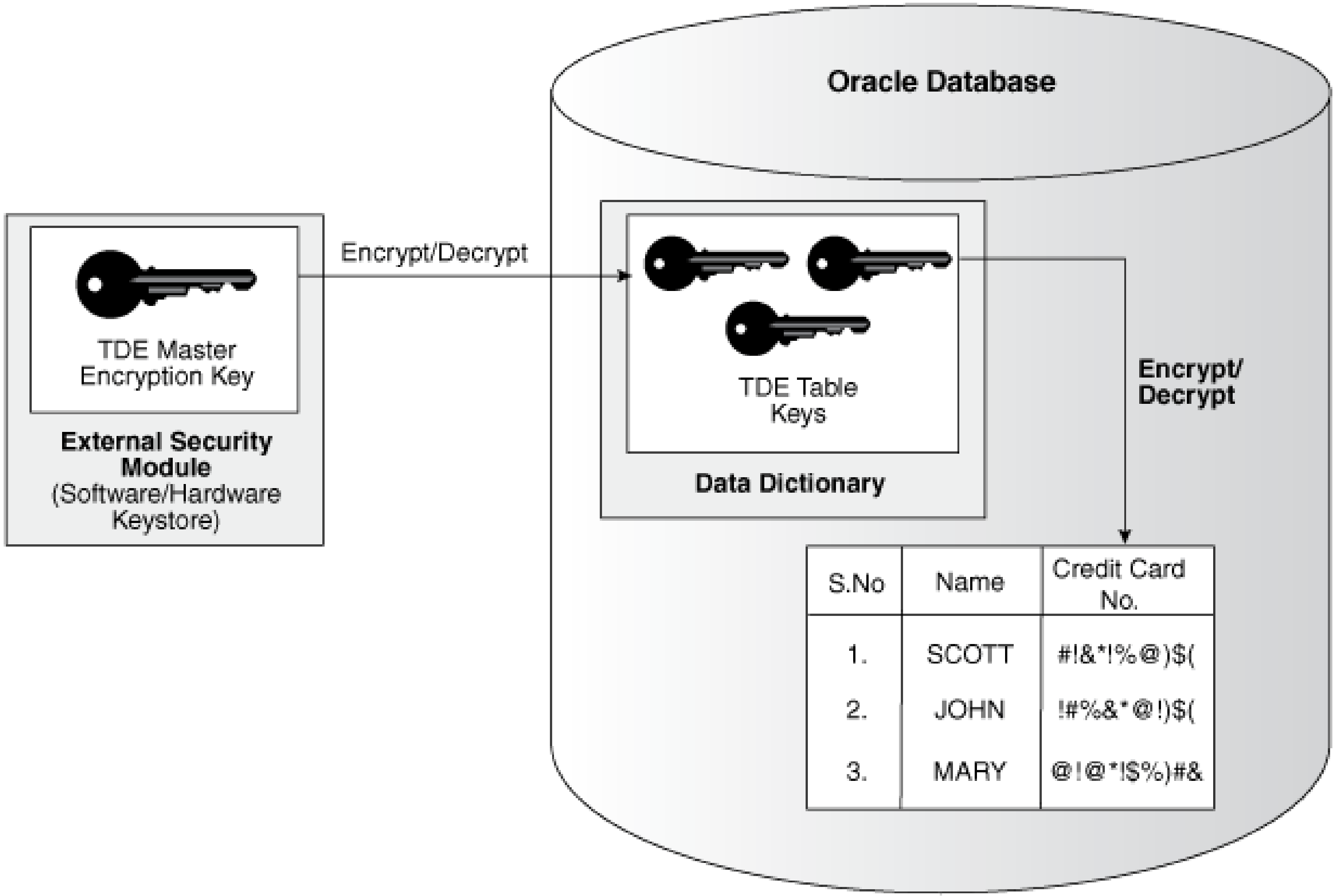
- Do not prevent users with sufficiently high privileges from accessing data (do not mix up with Oracle Database Vault)

- TDE does prevent operating system users with sufficient priviliges from access any data

- No additional storage needed on the compute nodes

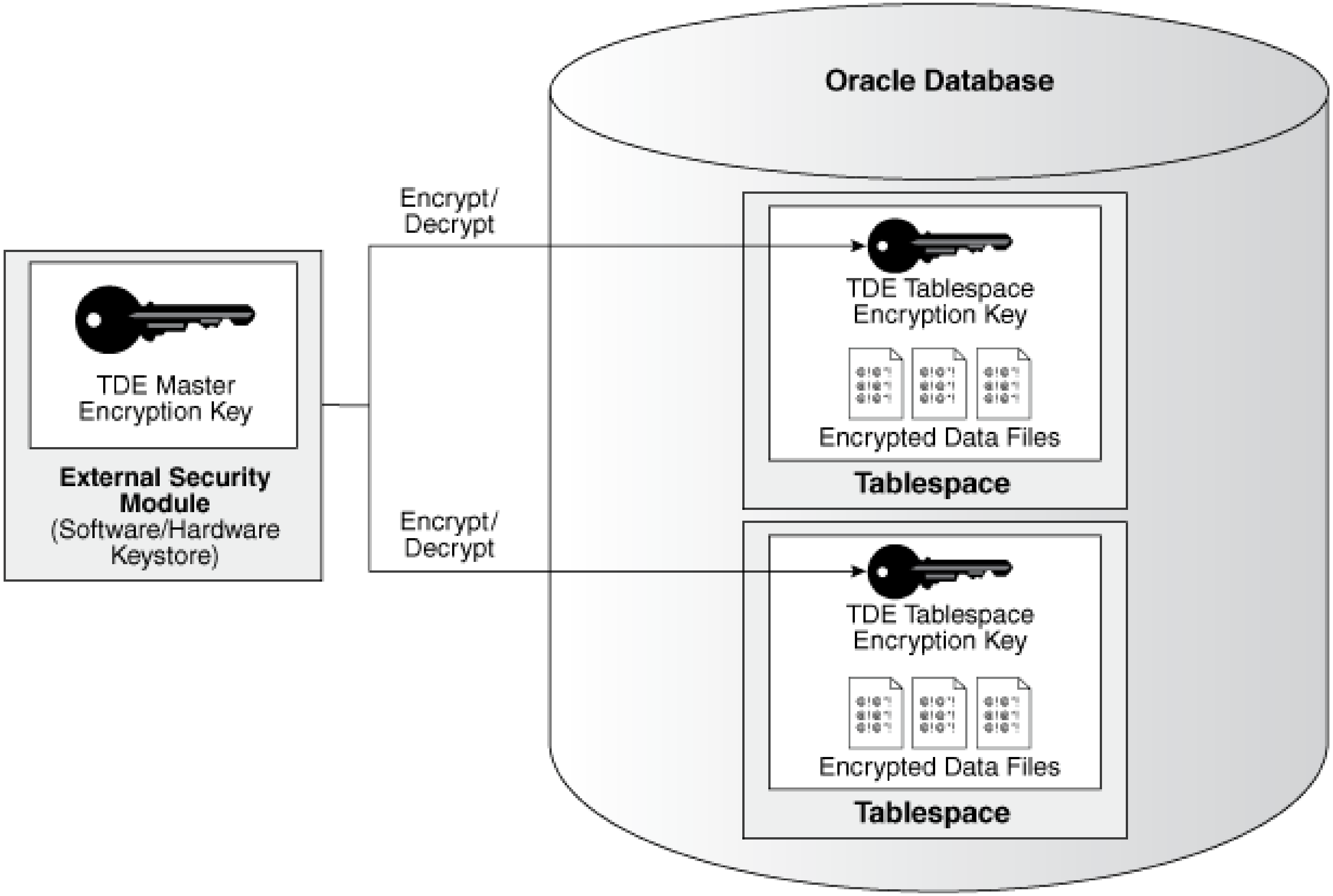
- Below RDBMS version 12.2 the tablespaces SYSTEM, SYSAUX, UNDO and TEMP cannot be encrypted. However, user data in UNDO, TEMP tablespaces and redo information is encrypted using TDE tablespace encryption

Oracle TDE Column Encryption



S.No	Name	Credit Card No.
1.	SCOTT	#!&*!%@)$(
2.	JOHN	!#%&*@!)$(
3.	MARY	@!@*!$%)#&

Oracle TDE Tablespace Encryption



Transparent Data Encryption

Allianz standard

- Tablespace encryption
- AES256 only accepted encryption method
- Key cannot be stored on the same location as data

Tablespace Encryption

11.2 export / import tablespaces

Offline operation

12.1 ALTER command with online switch

Semi online operation

19c with alter tablespace commands

Fully online

```
alter tablespace <TS_NAME> encryption online using 'aes256' encrypt;
```

ASFC vs. DBFS encryption

	ACFS		DBFS	
	non-enc	enc	non-enc	enc
read original GI	178,2MB/s	36,6MB/s	62MB/s	61MB/s
write original GI	41,4MB/s	7,9MB/s	47MB/s	46MB/s
read 12c GI with 28278811	334MB/s	185MB/s		
write 12c GI with 28278811	123MB/s	39MB/s		
write 18.4 GI with 29229120	276MB/s	266MB/s		

Exadata Cloud Service

- Quarter Rack: Containing 2 compute nodes and 3 Exadata Storage Servers.

- Vitrual machines

- Diskgroups

  DATA

  RECO

  ACFS

  DBFS

EXACS command line utilites

Dbaascli

Supports a variety of life-cycle and administration operations-Database Patching, SW library Updates, Oracle Home maintenance, PDB operations, TDE Management etc

OCI CL

Almost all of the operations which can be performed from console –Database System Launch, DB creation/deletion VCN and related resource operation, CPU scaling etc

Exacli

Used to execute specific cellclicommands from compute node to the Exadata Storage Servers that are associated with yourExaCSenvironment. Use case is for getting Storage Cell metrices and diagnostics info.

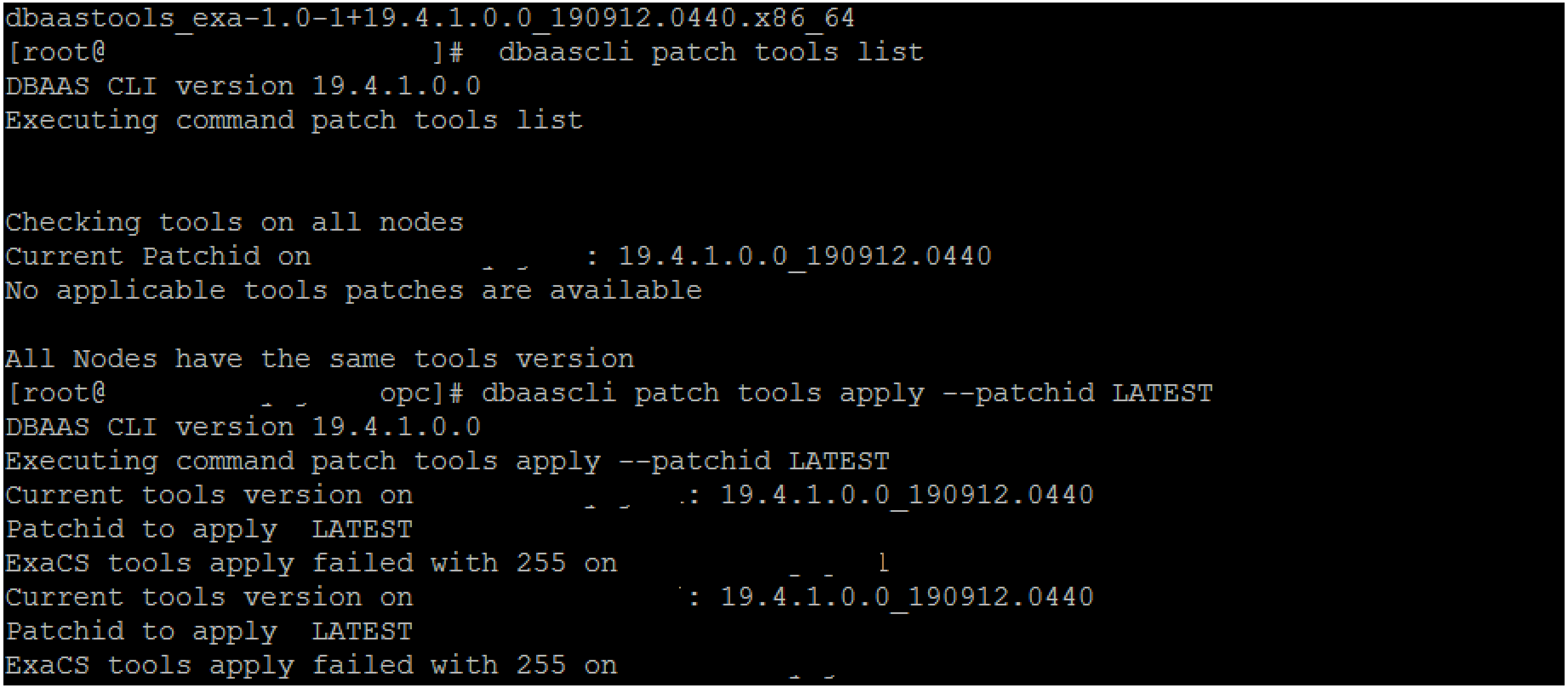
Dbaasapi

Manual Database operations, though recommended method is to use OCI CL or console for DB tasks such as DB creation & deletion.

bkup_api

Supports Backup life cycle –Creating configuration, Changing configuration, Backup, restore operations

Updating Cloud Tooling

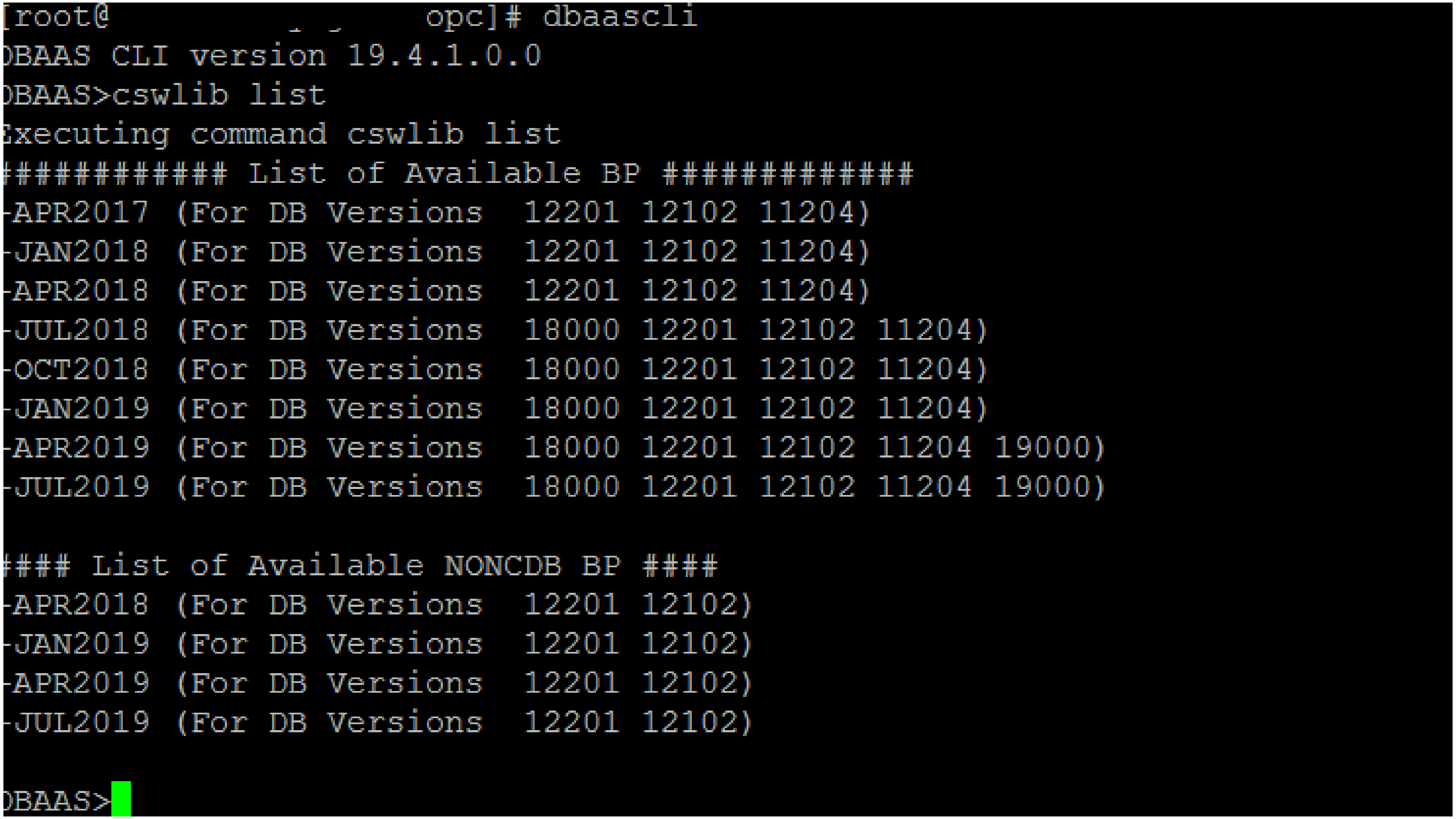


```
dbaastools_exa-1.0-1+19.4.1.0.0_190912.0440.x86_64
[root@[redacted]]#  dbaascli patch tools list
DBAAS CLI version 19.4.1.0.0
Executing command patch tools list


Checking tools on all nodes
Current Patchid on [redacted]: 19.4.1.0.0_190912.0440
No applicable tools patches are available

All Nodes have the same tools version
[root@[redacted] opc]# dbaascli patch tools apply --patchid LATEST
DBAAS CLI version 19.4.1.0.0
Executing command patch tools apply --patchid LATEST
Current tools version on [redacted]: 19.4.1.0.0_190912.0440
Patchid to apply  LATEST
ExaCS tools apply failed with 255 on [redacted]
Current tools version on [redacted]: 19.4.1.0.0_190912.0440
Patchid to apply  LATEST
ExaCS tools apply failed with 255 on [redacted]
```

Create Database in EXACS



```
[root@[redacted]opc]# dbaascli
DBAAS CLI version 19.4.1.0.0
DBAAS>cswlib list
Executing command cswlib list
############ List of Available BP #############
-APR2017 (For DB Versions  12201 12102 11204)
-JAN2018 (For DB Versions  12201 12102 11204)
-APR2018 (For DB Versions  12201 12102 11204)
-JUL2018 (For DB Versions  18000 12201 12102 11204)
-OCT2018 (For DB Versions  18000 12201 12102 11204)
-JAN2019 (For DB Versions  18000 12201 12102 11204)
-APR2019 (For DB Versions  18000 12201 12102 11204 19000)
-JUL2019 (For DB Versions  18000 12201 12102 11204 19000)

#### List of Available NONCDB BP ####
-APR2018 (For DB Versions  12201 12102)
-JAN2019 (For DB Versions  12201 12102)
-APR2019 (For DB Versions  12201 12102)
-JUL2019 (For DB Versions  12201 12102)

DBAAS>
```

Create Database in EXACS

```
cd /home/oracle/dbinput/
[root@*********** dbinput]# cat createdb.json
{
    "object": "db",
    "action": "start",
    "operation": "createdb",
    "params": {
        "nodelist": "",
        "cdb": "no",
        "bp": "JAN2019",
        "dbname": „DBNAME",
       "ohome_name" : "OraHome105_12102_dbbp190115_0",
        "edition": "EE_EP",
        "version": "12.1.0.2",
        "adminPassword": „***********",
        "charset": "AL32UTF8",
        "ncharset": "AL16UTF16",
        "backupDestination": "OSS",
        "cloudStorageContainer": "https://example.com/v1/something001/DB-BACKUP-NON-PROD-DBNAME",
        "cloudStorageUser": „********",
        "cloudStoragePwd": „*************"
    },
    "outputfile": "/home/oracle/dbinput/createdb.out",
    "FLAGS": ""
}
[root@*********** dbinput]#  /var/opt/oracle/dbaasapi/dbaasapi -i createdb.json
```

Create Database in EXACS

```
[root@************** dbinput]# cat createdb.out

{
   "msg" : "For security please remove your input file.",
   "object" : "db",
   "status" : "Starting",
   "errmsg" : "",
   "outputfile" : "/home/oracle/dbinput/createdb.out",
   "pid" : "",
   "action" : "start",
   "id" : "130",
   "operation" : "createdb",
   "logfile" : "/var/opt/oracle/log/DBNAME/dbaasapi/db/createdb/130.log"
}
```

Create Database in EXACS

```
[root@****** dbinput]# /var/opt/oracle/dbaasapi/dbaasapi -i
createdbStatus.json
```

```
[root@oce01-u6-ykj6v1 dbinput]# cat createdbStatus.json
{
  "object": "db",
  "action": "status",
  "operation": "createdb",
  "id": 130,
  "params": {
  "dbname": „DBNAME"
  },
"outputfile": "/home/oracle/dbinput/createdbStatus.out",
"FLAGS": ""
}
```

Create Database in EXACS

```
root@oce01-u6-ykj6v1 dbinput]# cat createdbStatus.out

{
   "msg" : "",
   "object" : "db",
   "status" : "Failed",
   "errmsg" : "Non-zero return from ocde: WARN : Parameter nid_tar_190 is not a valid parameter. Please
check the usage\\n\\nWARN : Parameter nid_tar_122_atp is not a valid parameter. Please check the
usage\\n\\nWARN : Parameter nid_tar_190_atp is not a valid parameter. Please check the usage\\nERROR :
expected file /var/opt/oracle/dbaas_acfs/db12102_bits_EXA.tar.gz not found\\nERROR : Assistant prep has
failed, please check ocde logfile /var/opt/oracle/log/TDE121T/ocde/ocde_2019-06-
24_14:26:13.61056558212.log\\nINFO: Total time taken by ocde is 75 seconds \\n\\n#### Completed OCDE
with errors, please check logs ####\\nINFO : ocde_time_format is 2019/06/24 14:26:12 \\n",
   "outputfile" : "/home/oracle/dbinput/createdb.out",
   "pid" : "58191",
   "action" : "start",
   "id" : "130",
   "operation" : "createdb",
   "logfile" : "/var/opt/oracle/log/DBNAME/dbaasapi/db/createdb/130.log"
}
```

Creating non-CDB databases using Oracle Database 12c on the Exadata Cloud Service (Doc ID 2528257.1)

Backup in EXACS

bkup_api is part of dbaas rpm, it is a python script

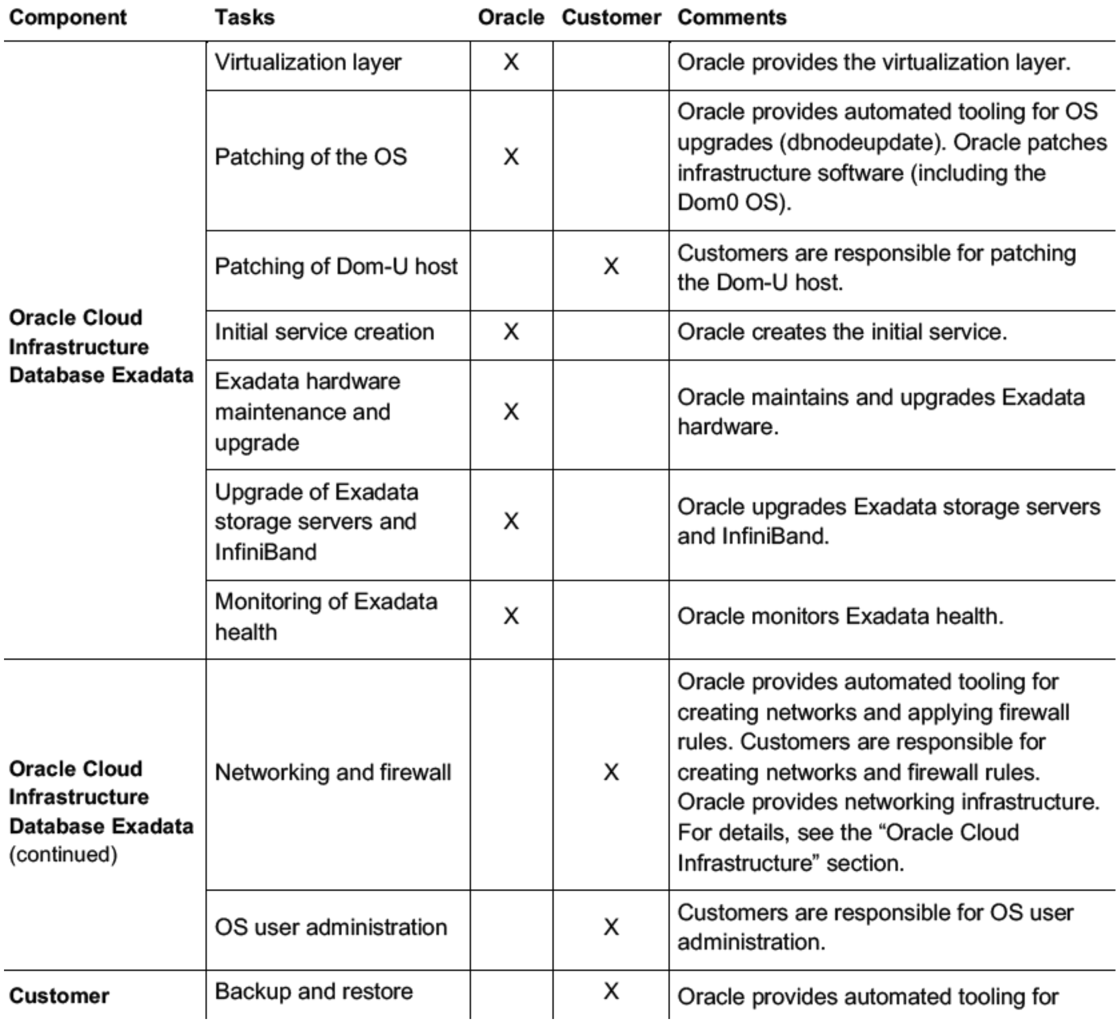
Create entryies in crontab, all nodes of the cluster

Backup to Object Store

SQLite database

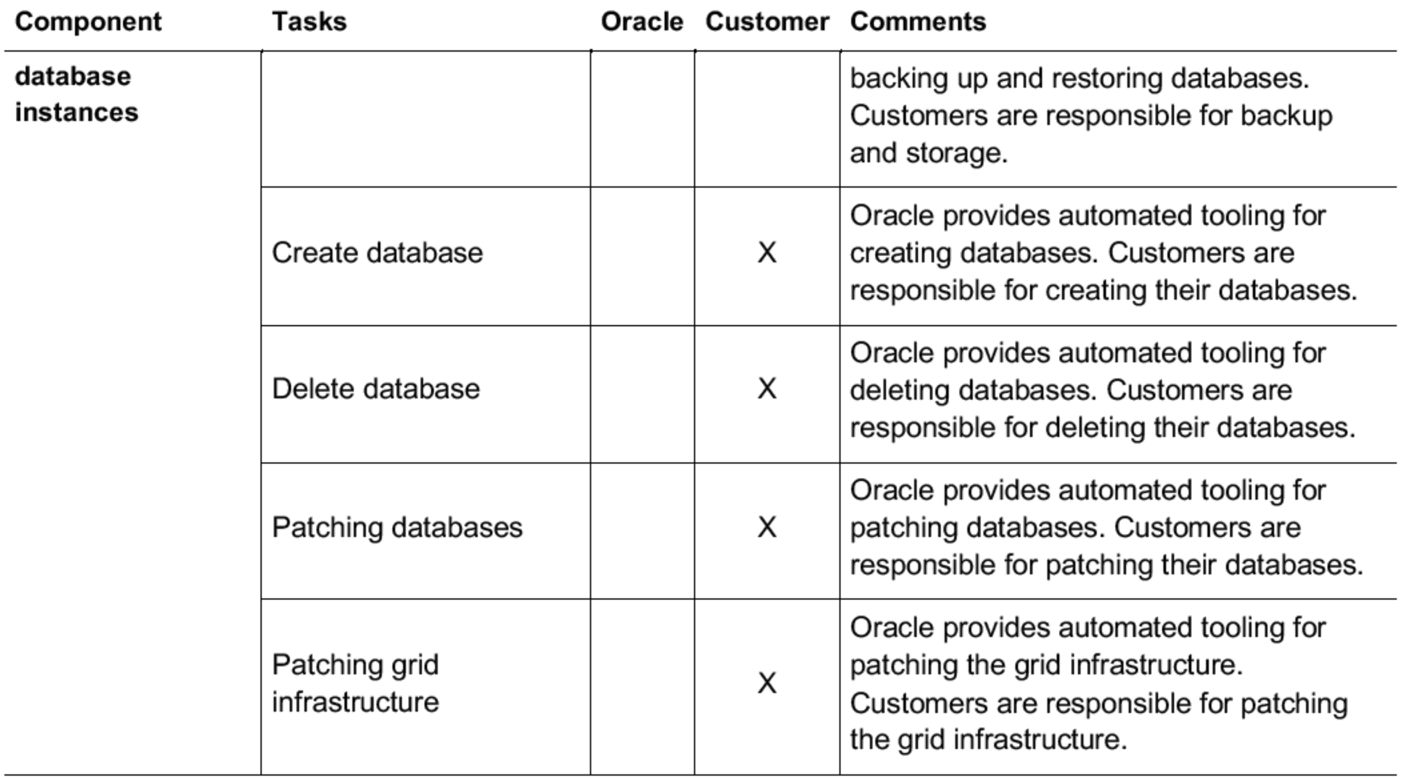
Compatibility problems with OKV

EXACS responsibilities



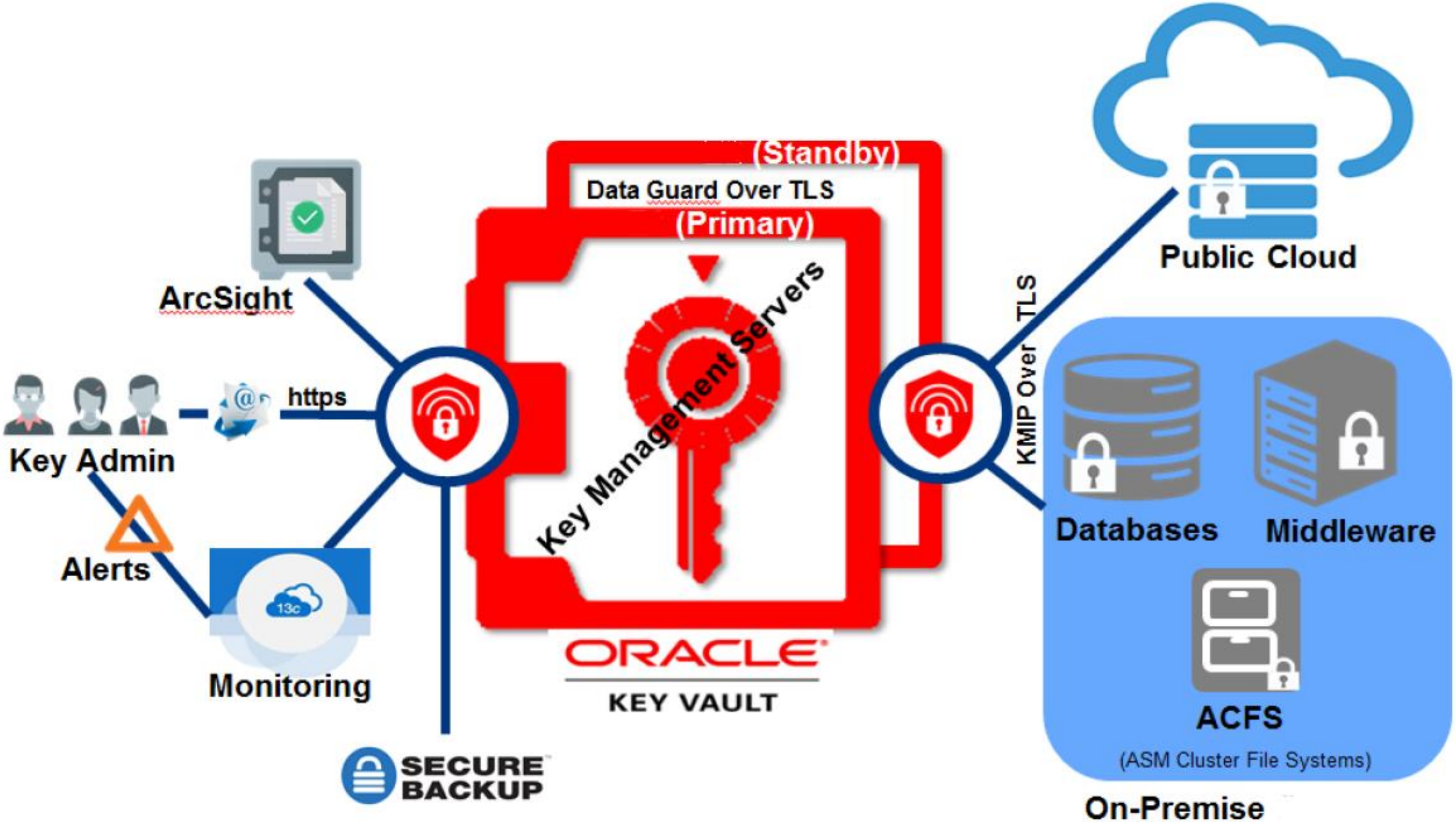
Component	Tasks	Oracle	Customer	Comments
Oracle Cloud Infrastructure Database Exadata	Virtualization layer	X		Oracle provides the virtualization layer.
	Patching of the OS	X		Oracle provides automated tooling for OS upgrades (dbnodeupdate). Oracle patches infrastructure software (including the Dom0 OS).
	Patching of Dom-U host		X	Customers are responsible for patching the Dom-U host.
	Initial service creation	X		Oracle creates the initial service.
	Exadata hardware maintenance and upgrade	X		Oracle maintains and upgrades Exadata hardware.
	Upgrade of Exadata storage servers and InfiniBand	X		Oracle upgrades Exadata storage servers and InfiniBand.
	Monitoring of Exadata health	X		Oracle monitors Exadata health.
Oracle Cloud Infrastructure Database Exadata (continued)	Networking and firewall		X	Oracle provides automated tooling for creating networks and applying firewall rules. Customers are responsible for creating networks and firewall rules. Oracle provides networking infrastructure. For details, see the "Oracle Cloud Infrastructure" section.
	OS user administration		X	Customers are responsible for OS user administration.
Customer	Backup and restore		X	Oracle provides automated tooling for

EXACS responsibilities



Component	Tasks	Oracle	Customer	Comments
database instances				backing up and restoring databases. Customers are responsible for backup and storage.
	Create database		X	Oracle provides automated tooling for creating databases. Customers are responsible for creating their databases.
	Delete database		X	Oracle provides automated tooling for deleting databases. Customers are responsible for deleting their databases.
	Patching databases		X	Oracle provides automated tooling for patching databases. Customers are responsible for patching their databases.
	Patching grid infrastructure		X	Oracle provides automated tooling for patching the grid infrastructure. Customers are responsible for patching the grid infrastructure.

Oracle Key Vault



OKV config

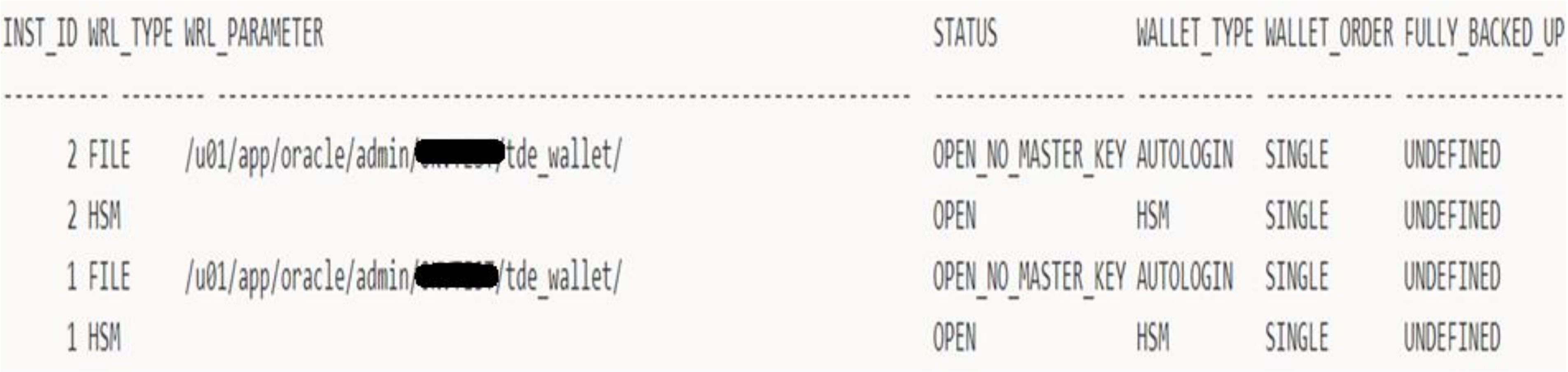
1. Create the OKV client install jars for the database
2. Install the OKV client for the database
3. Database environment and properties configuration
4. Cluster properties
5. SQLNET.ORA configuration
6. Open the wallet
7. Create the first master encryption key and configure AUTO OPEN.

Endpoint client configuration

okvclient.ora file

```
SERVER=XX.XX.XX.XX:port
STANDBY_SERVER=XX.XX.XX.XX:port
CONF_ID=ITz82WHtMXTxAzlZ
SERVER_DN=CN=server_cert,OU=Key_Vault,O=Oracle,L=Redwood_City,ST=California,C=us
GEN_TIMESTAMP=2019-08-19 13\:21\:56 UTC
UPDATE_TIMESTAMP=2019-08-22 15\:47\:45.304 UTC
SW_TYPE=ENROLLED_ENDPOINT_SOFTWARE
JAVA_HOME=/usr/java/latest/
OKV_JVM_LIB_PATH=/usr/java/latest/jre/lib/amd64/server/libjvm.so
EP_TYPE=UNKNOWN
OKV_HOSTNAME=okv.domain
SERVER_POLL_TIMEOUT=300.00
SSL_WALLET_LOC=/u02/app/oracle/okvclient/DBNAME/ssl
_NOT_STRICT_PKCS11=1
PKCS11_NO_KMIP_OBJECT_ACCESS_CHECK=0
PKCS11_CACHE_TIMEOUT=60.00
PKCS11_PERSISTENT_CACHE_TIMEOUT=240.00
PKCS11_PERSISTENT_CACHE_FIRST=1
PKCS11_PERSISTENT_CACHE_REFRESH_WINDOW=30.00
_TRACE_DIR=/u02/app/oracle/okvclient/DBNAME/conf/
_TRACE_LEVEL=16
```

Successful OKV configuration



```
INST_ID WRL_TYPE WRL_PARAMETER                                                  STATUS            WALLET_TYPE WALLET_ORDER FULLY_BACKED_UP
---------- -------- ------------------------------------------------------------ ----------------- ----------- ------------ ---------------
         2 FILE     /u01/app/oracle/admin/[redacted]/tde_wallet/                 OPEN_NO_MASTER_KEY AUTOLOGIN  SINGLE       UNDEFINED
         2 HSM                                                                    OPEN              HSM         SINGLE       UNDEFINED
         1 FILE     /u01/app/oracle/admin/[redacted]/tde_wallet/                 OPEN_NO_MASTER_KEY AUTOLOGIN  SINGLE       UNDEFINED
         1 HSM                                                                    OPEN              HSM         SINGLE       UNDEFINED
```

OKV and EXACS known issues

- Encryption and Compression → Increased backup volume
- CPU consumption increased by 5 -15 %
  - encryption compute node level
  - decryption storage cell level
- Lost master encryption key
- Yearly rekey operation

QUESTIONS?

THANK YOU FOR YOUR ATTENTION!