

Seguridad en Bases de Datos

PEC 1

Seguridad y pentesting de servidores de datos

UOC - MISTIC

Pablo Riutort Grande

12 de octubre de 2020

1.

1.1.

Una combinación roles para el escenario presentado podría ser el siguiente:

- **DBA (Administrador de Base de Datos):** Este rol permite definir el schema de la base de datos así como sus usuarios y los permisos de estos. También es el responsable de velar por la seguridad de la base de datos aplicando el plan de seguridad y backups y de reparar los posibles fallos debidos al hardware o al software.
- **Administrador de Sistemas:** Este rol es muy similar al anterior exceptuando la definición del schema de la base de datos. También vela por la seguridad de la base de datos y de sus procesos así como los backups y el acceso y disponibilidad a la BD por parte de los usuarios.
- **Miembro del departamento de contabilidad:** Este es un usuario normal con permisos restringidos a las tablas que gestionan y relacionan los usuarios con sus sueldos.

Los usuarios que podrían adquirir uno o varios de esos roles son los siguientes:

- **Usuario del departamento de contabilidad:** Este usuario tiene acceso y permisos de consulta y modificación sobre las tablas relacionadas con la contabilidad de la empresa y sus usuarios.
- **CSO:** El CSO es el Responsable de la Seguridad Corporativa. Su función principal es garantizar la seguridad física y la tecnológica.
- **Responsable de seguridad:** Se encarga de que el tratamiento de datos personales se realicen conforme al RGPD.
- **Personal de seguridad:** Sería la persona que velaría de la seguridad física, en este caso de los equipos, las cintas y su adecuado acceso y transporte.

1.2.

El plan director de seguridad (PDS) elaborado por el CSO y el Responsable de seguridad deberá ser seguido por todos los usuarios. Algunas de las medidas que puede definir son:

- **Control de acceso físico a las instalaciones:** Tarjetas de identificación que deberán llevarse colgadas en todo momento dentro del recinto de trabajo.
- **Control de acceso a los ordenadores:** Los equipos están protegidos por usuario y contraseña.
- **Control de acceso a los sistemas de la empresa:** Los accesos a servidores, bases de datos, intranets, etc. deberán ser gestionados mediante software adicional de control de acceso como una doble autenticación mediante una app, SSH, LDAP, etc.
- **Control de acceso a la red:** A la red se accede mediante la VPN de la empresa y el acceso a esta está gestionado por el equipo de seguridad o el departamento de IT. Podría recomendarse el uso de certificados digitales y SSL.
- **Cifrado de disco:** Los ordenadores deberán tener el disco cifrado.

- Control de dispositivos: En caso de traer un dispositivo o equipo externo deberá ser avalado por el departamento de IT y deberá cumplir con las especificaciones que se establezcan.
- Control de acceso a la base de datos: El DBS podría limitar el acceso a únicamente a través de equipos especiales o servidores jump que estén en una DMZ protegida por firewalls.
- Realización periódica de backups de los equipos personales y por parte del DBS o del sysadmin backups de las bases de datos.

1.3.

1.3.1.

El nuevo planteamiento supone un cambio significativo en la gestión de las bases de datos de la compañía ACME.

El rol de DBA pasa a ser responsabilidad de la compañía de Cloud Computing y desaparece, al menos para esta competencia, de la empresa ACME. El rol de administrador de sistema se mantiene pero este deberá adaptar las necesidades de acceso y seguridad hacia la plataforma de Cloud Computing ya que esta es la que ahora se encarga de la seguridad y acceso de los datos per se, deberá asegurar las conexiones y los posibles accesos a base de datos de manera segura entre ACME y Cloud Computing de la misma forma que lo hacía antes. Dependerá de él entender y evaluar los riesgos de la arquitectura de las dos empresas en este aspecto y velar porque la conexión sea lo más accesible y segura posible.

El rol de personal de contabilidad y otros usuarios de la base de datos tendrán las mismas responsabilidades sobre los datos pero deberán adaptarse a la nueva herramienta y quizá modificar algún flujo de trabajo; quizá deban autenticarse de otra forma o conectarse a otros servidores o servicios que permitan la conexión segura entre su ordenador y el cloud.

En cuanto a seguridad física, de transporte de las cintas y de acceso a los servidores desaparece y se libera al personal de seguridad de esta responsabilidad.

Finalmente, el plan de seguridad y tratamiento de los datos deberá actualizarse y coordinarse entre ambas compañías ya que muchas tareas de seguridad de los datos se han visto delegadas pero su uso responsable y acorde con las leyes vigentes sigue siendo responsabilidad de la empresa ACME.

1.3.2.

Parte de la seguridad queda externalizada al servicio de Cloud Computing, por tanto, ahora existe esa oportunidad de atacar directamente al servicio de Cloud Computing que es la delegada de la gestión de las bases de datos de ACME y de quizá otras compañías.

También surge la problemática de que el factor humano se multiplica por 2, es decir, hay 2 empresas implicadas en el tratamiento seguro de los datos y por tanto el riesgo se ve incrementado en este aspecto.

Surge la oportunidad de atacar una nueva conexión entre ACME y el servicio de Cloud Computing. Anteriormente la conexión a la base de datos estaba gestionada por una sola compañía, ahora hay 2 compañías implicadas y probablemente la de Cloud Computing tenga una arquitectura de seguridad para conexiones externas estandarizada y fácil de conocer y, por ende, de explotar; ahí reside el nuevo riesgo.

Finalmente, surge también el riesgo por parte de ACME que surgen a raíz de una posible plataforma de conexión que haya para acceder a la base de datos. Dicha plataforma puede ser un

nuevo foco de vulnerabilidades y además vendrá sumado al riesgo que supone para los empleados adaptarse al nuevo uso de manera segura.

1.3.3.

ACME deberá implantar un nuevo plan de seguridad que recoja y aglutine la herramienta que ofrezca la empresa de Cloud Computing para acceder a la base de datos. Esto incluye sesiones formativas a los usuarios finales para interactuar de manera segura y eficiente y diseñar e implementar una nueva arquitectura de conexión segura y compatible con ACME por parte del departamento de IT o el administrador de sistemas.

Medidas que deberá exigir ACME son las mismas que debía autoexigirse cuando los datos eran responsabilidad suya, que los datos sean accesibles y que se cumpla la normativa vigente en cuanto a su uso y tratamiento. También deberá exigir a la empresa de Cloud Computing que se tenga una información constante sobre noticias de interés que puedan repercutir en ACME tales como nuevas normativas, vulnerabilidades que se descubran y, por supuesto, que se informe en caso de brecha o algún otro evento de importancia que afecte directamente a los datos.

1.3.4.

Podría plantearse no externalizarse este servicio cuando los datos sean especialmente sensibles o se vean adscritos a sanciones muy graves en caso de fuga. También si los datos son muy valiosos o las necesidades de la empresa respecto a ellos no se adaptan completamente a lo que ofrezca ninguna plataforma de Cloud Computing.

Finalmente, también podría no plantearse esta externalización si el coste de la misma, bien económico o de recursos, no valga la pena a mantener el esquema actual.

1.4.

En el cluster se han creado 3 usuarios cada uno con un rol diferente.

Database Access

Database Users

Custom Roles

+ ADD NEW DATABASE USER










User Name	Authentication Method	MongoDB Roles	Resources	Actions
 user_0	SCRAM	database_manager@admin	All Resources	 EDIT  DELETE
 user_1	SCRAM	sys_admin@admin	All Resources	 EDIT  DELETE
 user_3	SCRAM	contable@admin	All Resources	 EDIT  DELETE

Figura 1: Usuarios del cluster

El rol de DBA tiene todos los permisos posibles sobre la base de datos.

Role Name ↕	Granted Actions and Roles	
database_manager	useUUID	@all databases (all collections)
	listSessions	@all databases (all collections)
	killAnySession	@all databases (all collections)
	connPoolStats	@all databases (all collections)
	listDatabases	@all databases (all collections)
	serverStatus	@all databases (all collections)
	top	@all databases (all collections)
	find	@db (col)
	insert	@db (col)
	remove	@db (col)
	update	@db (col)
	bypassDocumentValidation	@db (col)
	createCollection	@db (col)
	createIndex	@db (col)
	dropCollection	@db (col)
	changeStream	@db (col)
	collMod	@db (col)
	compact	@db (col)
	convertToCapped	@db (col)
	dropIndex	@db (col)
	reIndex	@db (col)
	collStats	@db (col)
	dbHash	@db (col)
	listIndexes	@db (col)
	validate	@db (col)
	enableProfiler	@db (all collections)
	dropDatabase	@db (all collections)
	renameCollectionSameDB	@db (all collections)
	dbStats	@db (all collections)
	listCollections	@db (all collections)
	dbAdminAnyDatabase	@admin
	readWriteAnyDatabase	@admin
	readWrite	@db
	dbAdmin	@db
	read	@db
	readAnyDatabase	@admin
	clusterMonitor	@admin
	backup	@admin
	enableSharding	@admin

Figura 2: Rol de DBA

El rol de sys.admin tiene todos los permisos posibles sobre la base de datos excepto los que modifican el schema de la misma. También se incluye el rol de contable que tiene permisos de CRUD sobre la colección de nóminas y buscar y actualizar sobre la colección de usuarios.

sys_admin	enableProfiler	@db (all collections)
	dropDatabase	@db (all collections)
	renameCollectionSameDB	@db (all collections)
	dbStats	@db (all collections)
	listCollections	@db (all collections)
	useUUID	@all databases (all collections)
	listSessions	@all databases (all collections)
	killAnySession	@all databases (all collections)
	connPoolStats	@all databases (all collections)
	listDatabases	@all databases (all collections)
	serverStatus	@all databases (all collections)
	top	@all databases (all collections)
	dbAdminAnyDatabase	@admin
	readWriteAnyDatabase	@admin
	readWrite	@db
	dbAdmin	@db
	read	@db
	readAnyDatabase	@admin
	clusterMonitor	@admin
	backup	@admin
	enableSharding	@admin
contable	find	@db (nominas) @db (usuarios)
	insert	@db (nominas)
	remove	@db (nominas)
	update	@db (nominas)
		@db (usuarios)
	bypassDocumentValidation	@db (nominas)

Figura 3: Roles de administrador de sistemas y de contable

Algunas de las medidas de seguridad especificadas anteriormente se pueden incorporar, por ejemplo la de acceder a la base de datos desde equipos o servidores específicos [Fig 4] o acceder con credenciales también es posible mediante el uso de LDAP y también se ofrece el encriptado del cluster securizando así el disco [Fig 5].

Network Access

IP Access List Peering Private Endpoint

[+ ADD IP ADDRESS](#)

You will only be able to connect to your cluster from the following list of IP Addresses:

IP Address	Comment	Status	Actions
<input type="text" value="address"/> (includes your current IP address)	jump_server1	Active	EDIT DELETE

Figura 4: Restringir el acceso a unas IPs específicas

Advanced

LDAP Authentication cannot be configured without an active dedicated cluster running MongoDB 3.6 or higher.

LDAP Authentication ☐ OFF

Enabling LDAP authentication allows users to login to dedicated Atlas clusters using credentials that are verified by a LDAP server you control. Each user that has access to the databases, and their privileges after authenticating, are configured under the "MongoDB Users" tab.

Turning on this feature will increase your daily cluster pricing. [Read more.](#)

LDAP Authorization (LDAP Authentication required) ☐ OFF

LDAP Authorization simplifies the management of a large number of users by allowing control at the LDAP group level. LDAP groups can be added under the "MongoDB Users" tab and given a single set of privileges. All users in that LDAP group can then authenticate to Atlas clusters with those privileges.

Encryption at Rest using your Key Management ☐ OFF

Provide your AWS Key Management Service (AWS KMS), Azure Key Vault, or Google Cloud KMS encryption key details to enable Encryption at Rest with the WiredTiger™ Encrypted Storage Engine.

Turning on this feature will increase your daily cluster pricing. [Read more.](#)

Figura 5: Medidas de acceso avanzadas

2.

Para la realización de este ejercicio y debido a algunas dificultades técnicas se ha utilizado la imagen oficial de Oracle Database 12c para Docker [1] en Ubuntu 20.04 LTS. Docker nos permite desplegar aplicaciones dentro de estructuras virtuales, en este caso, Oracle Database 12c [2] desde la terminal:

```
1 docker run -d
2   --name oracle1
3   -p 1521:1521 -p 5500:5500
4   -e ORACLE_SID=DEV
5   -e ORACLE_PDB=TRUNK
6   -e ORACLE_PWD=Database3
7   -e ORACLE_CHARACTERSET=AL32UTF8
8   store/oracle/database-enterprise:12.2.0.1

1 docker exec -it oracle1 bash -c "source /home/oracle/.bashrc; sqlplus sys/
   Oradoc_db1@ORCLCDB as sysdba"
```

2.1.

Para ver las Bases de Datos que hay creadas por defecto podemos listarlas con la query:

```
1 SQL> SELECT TABLESPACE_NAME FROM DBA_TABLESPACES;
```

```
SQL> SELECT TABLESPACE_NAME FROM DBA_TABLESPACES;

TABLESPACE_NAME
-----
SYSTEM
SYSAUX
UNDOTBS1
TEMP
USERS
```

Figura 6: Query para mostrar tablas por defecto

2.2.

Un componente importante de una base de datos de Oracle es su diccionario de datos (*data dictionary*), que se trata de un conjunto de tablas de solo lectura que proporciona metadatos de la base de datos. El contenido del diccionario de datos se divide en Base Tables que guardan información sobre la misma base de datos y cuyo acceso lectura/escritura está restringido a la propia base de datos y Views que decodifica las base tables en información inteligible para el usuario [3].

De este último conjunto se podrían destacar el siguiente subconjunto de tablas que contienen información relevante.

- Vistas con prefijo ALL_: Objetos sobre los que un usuario tiene privilegios
- Vistas con prefijo USER_: Objetos que pertenecen a un usuario.
- Vistas con prefijo DBA_: Contiene todos los objetos con información útil para el administrador. Su uso está restringido al administrador de la base de datos.

2.3.

Para saber los usuarios que se crean por defecto en la base de datos podemos hacer una consulta sobre la tabla DBA_USERS que contiene información sobre los usuarios de la base de datos [Fig. 7].

Para inspeccionar los roles de los usuarios, podemos consultar la tabla DBA_SYS_PRIVS y hacer una JOIN con la tabla DBA_USERS de la siguiente manera:

```
1 SELECT USERNAME, PRIVILEGE FROM DBA_USERS INNER JOIN DBA_SYS_PRIVS ON DBA_USERS.
   USERNAME = DBA_SYS_PRIVS.GRANTEE ORDER BY DBA_USERS.USERNAME;
```

Sin embargo, esta query genera un resultado de 472 filas, así que se mostrarán los permisos del usuario SYSTEM que tan solo goza de 8 privilegios [Fig. 8].


```

SQL> SELECT * FROM DICTIONARY WHERE TABLE_NAME = 'DBA_USERS';

TABLE_NAME
-----
COMMENTS
-----
DBA_USERS
Information about all users of the database

SQL> SELECT USERNAME FROM DBA_USERS;

USERNAME
-----
SYS
SYSTEM
XS$NULL
OJVMSYS
LBACSYS
OUTLN
SYSSUMF
DBSNMP
APPOSSYS
DBSFUSER
GGSYS

USERNAME
-----
ANONYMOUS
FLOWS_FILES
CTXSYS
SI_INFORMTN_SCHEMA
DVSYS
DVF
GSMADMIN_INTERNAL
ORDPLUGINS
APEX_050000
MDSYS
OLAPSYS

USERNAME
-----
ORDDATA
XDB
WMSYS
ORDSYS
GSMCATUSER
MDDATA
SYSBACKUP
REMOTE_SCHEDULER_AGENT
GSMUSER
APEX_PUBLIC_USER
SYSRAC

USERNAME
-----
AUDSYS
DIP
SYSKM
ORACLE_OCM
SYSDG
SPATIAL_CSW_ADMIN_USR

39 rows selected.

```

Figura 7: Query para mostrar información de DBA_USERS y query para mostrar los usuarios de DBA_USERS

```
SQL> SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'SYSTEM';

PRIVILEGE
-----
CREATE MATERIALIZED VIEW
CREATE TABLE
UNLIMITED TABLESPACE
GLOBAL QUERY REWRITE
MANAGE ANY QUEUE
ENQUEUE ANY QUEUE
SELECT ANY TABLE
DEQUEUE ANY QUEUE

8 rows selected.
```

Figura 8: Query para mostrar los permisos del usuario SYSTEM

2.4.

Los puertos a la escucha son el 1521 (Oracle TNS Listener) que pasa las peticiones de un usuario a la instancia de la base de datos a través de la red y el 5500 (OEM Database Express) es una herramienta web incluida en Oracle Database 12c que sirve para administrar distintas áreas de la BD (Configuración, Almacenamiento, Seguridad y Rendimiento) [4] [5].

```
pablo@fossa:~$ docker port oracle1
1521/tcp -> 0.0.0.0:1521
5500/tcp -> 0.0.0.0:5500
```

Figura 9: Listado de puertos activos del container de Oracle Database

Para deshabilitarlos se puede usar el comando “lsnrctl” [7]:

```
1 lsnrctl STOP [listener_name]
```

2.5.

Los binarios, dentro de la imagen de Docker, se encuentran en el directorio /u01/app/oracle/product/12.2.0/dbhome_1/bin. [Fig. 10].

Los archivos de datos, en cambio, se encuentran en /ORCL/u02/app/oracle/oradata/ORCLCDB [6] [Fig. 11].

```

[oracle@7d45ac71bb46 bin]$ pwd
/u01/app/oracle/product/12.2.0/dbhome_1/bin
[oracle@7d45ac71bb46 bin]$ ls
acfsroot          dbupgrade         hsalloct         mkstore           oraenv            sqldeveloper.sh
adapters          dbv               hsdepexa         mkstore.bat       orajaxb           sqldr
adrci             deploync         hsots            mtactl            orald             sqlplus
afdboot          dg4odbc          imp              ncomp             oraping           srvconfig
afddriverstate   dg4pwd           impdp            netca             orapltpe          srvctl
afdrout           dgmgri           jssu             netca_deinst.sh  orapkl            statusnc
afdttool          diagsetup        kfed             netmgr            orapkl.bat        symfind
afdttool.bin     diskmon.bin      kfod             nid               orapwd            sysresv
agtctl            dropjava         kfod.bin         odisrvreg         oraxml            tkprof
amdu             dsm12ldif        kgmgr            oerr              oraxsl            tnnfg
aqxmctl           dumpsga          lbuilder         oerr.pl           orlon             tnslnr
aqxmctl.pl        echodo           lcscan           oidca             osdbagrp          tnsping
asmcmd            emca             ldapadd          oldprovtool        osh              transx
asmcmdcore        emdwgrd          ldapaddmt        ojvmjava          ott               trcasst
bndlchk           emdwgrd.pl       ldapbind         ojvmtc            owm              trcldr
chopt             eusm             ldapcompare      okaroot           patchgen          trcroute
chopt.ini         exp              ldapdelete       okcreate          platform_common  trcssess
chopt.pl          expdp            ldapmoddn        okdstry           plshprof          tstshm
cluvfy            extjob           ldapmodify        okinit            proc              uidrvcl
cluvfyexec.sh     extjobo          ldapmodifymt      oklist            procob            umu
coraenv           extproc          ldapsearch        olfscmd           rawutil           unzip
crsdiag.pl        extusrupgrade    ldifmigrator     olfsroot          rconfig           wrap
ctxkbt           fmpu            linkshlib         olsadmintool       relink            wrc
ctxlc             fmpu            lmsgen           olsoidsync         renamedg          xml
ctxload           genagtsh         loadjava          onsctl             roohctl           xmlcg
cursize           genclntsh        loadpsp           oputil            rtsora            xmldiff
dbca              genclntst        lsnodes          orabase            sbttest           xmlw
dbfs_client       genezi           lsnrctl          orabaseconfig      schagent          xsl
dbfs_size         genksms          lxchknlb         orabasehome        schema            xsq
dbgeu_run_action.pl gennfgt          lxege            oracg              schemasync        xvm
dbhome            gennttab         lxinst           oracle             setasmgid         zip
dbshut            genoccish        mapsga           oradism            skgxpinfo
dbstart           genoradksh       maxmem           oradnfs            sql
dbua              gensyslib        mkpatch          oradnfs_run.sh

```

Figura 10: Archivos binarios de Oracle Database.

```

[oracle@7d45ac71bb46 ORCLCDB]$ pwd
/ORCL/u02/app/oracle/oradata/ORCLCDB
[oracle@7d45ac71bb46 ORCLCDB]$ ls -R
.:
cntrlORCLCDB.dbf  pdbseed          system01.dbf  undotbs01.dbf
orclpdb1         sysaux01.dbf    temp01.dbf   users01.dbf

./orclpdb1:
sysaux01.dbf  system01.dbf  temp012017-03-02_07-54-38-075-AM.dbf  undotbs01.dbf  users01.dbf

./pdbseed:
sysaux01.dbf  system01.dbf  temp012017-03-02_07-54-38-075-AM.dbf  undotbs01.dbf

```

Figura 11: Archivos de datos de Oracle Database.

2.6.

Los procesos relacionados con Oracle Database en el container se ejecuta con el usuario “oracle” con un PID muy elevado [Fig. 12].

```
[oracle@7d45ac71bb46 /]$ ps -exo user,pid,ppid,ni,comm
USER      PID     PPID    NI  COMMAND
oracle      1         0     0   bash
oracle     22         1     0  ora_pmon_orclcd
oracle     24         1     0  ora_clmn_orclcd
oracle     26         1     0  ora_psp0_orclcd
oracle     28         1     0  ora_vktm_orclcd
oracle     32         1     0  ora_gen0_orclcd
oracle     34         1     0  ora_mman_orclcd
oracle     38         1     0  ora_scmm_orclcd
oracle     42         1     0  ora_diag_orclcd
oracle     44         1     0  ora_scmm_orclcd
oracle     48         1     0  ora_dbrm_orclcd
```

Figura 12: Procesos de Oracle en el container

2.7.

Durante el proceso de instalación mediante el instalador, en el primer paso llamado “Configure Security Updates”, nos permite introducir una dirección de correo electrónico en el que recibir notificaciones de seguridad. Más adelante, en el paso llamado “Typical Installation”, nos permite especificar la contraseña que usarán los usuarios SYS, SYSTEM, SYSMAN y DBSNMP [8].

2.8.

La instalación de MongoDB Community Server se ha hecho a través del gestor de paquetes dpkg sobre el paquete mongodb-org-server_4.4.1_amd64.deb y no ha habido ninguna opción de seguridad disponible. Sin embargo, existe un archivo de configuración para mongo, /etc/mongo.conf, con un apartado de seguridad [Fig. 13].

```

pablo@fossa:~/Downloads$ cat /etc/mongod.conf
# mongod.conf

# for documentation of all options, see:
#   http://docs.mongodb.org/manual/reference/configuration-options/

# Where and how to store data.
storage:
  dbPath: /var/lib/mongodb
  journal:
    enabled: true
# engine:
# mmapv1:
# wiredTiger:

# where to write logging data.
systemLog:
  destination: file
  logAppend: true
  path: /var/log/mongodb/mongod.log

# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

# how the process runs
processManagement:
  timeZoneInfo: /usr/share/zoneinfo

#security:

#operationProfiling:

#replication:

#sharding:

## Enterprise-Only Options:

#auditLog:

#snmp:

```

Figura 13: Archivos de configuración de MongoDB.

Por defecto, la seguridad no está aplicada pero en Mongo existen distintas configuraciones para este parámetro [Fig. 14]

```

pablo@fossa:~/Downloads$ grep security -A 1 /etc/mongod.conf
security:
  authorization: enabled

```

Figura 14: Sección de seguridad en /etc/mongo.conf

Con esta configuración se activa el RBAC y de manera implícita la autenticación [9].

2.9.

El puerto por defecto para instancia de mongo y el mongo daemon es el 27017. Existen otros puertos relacionados con la configuración de mongo en modo cluster los 27018 y el 27019 [10]. Para usar otro puerto se puede editar el archivo /etc/mongo.conf en el apartado de “net” [Fig. 15].

```
pablo@fossa:~$ grep network -A 3 /etc/mongod.conf
# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1
```

Figura 15: Sección de network en /etc/mongod.conf

2.10.

El proceso de mongod ha sido ejecutado por el usuario mongodb y con un PID igual a 1.

```
root@1907e805c66d:/# ps -eao user,pid,ppid,ni,comm
USER      PID    PPID  NI COMMAND
mongodb    1       0    0 mongod
```

Figura 16: Procesos de Mongo en el container

2.11.

Tanto los binarios como los archivos de datos se encuentran en /data/db donde podemos encontrar el Storage Engine de WiredTiger, los índices y colecciones de la base de datos y el journaling que mantiene un registro de las operaciones del storage engine [11]

```
root@1907e805c66d:/data/db# ls -l
total 272
-rw-r----- 1 mongodb mongodb  47 Oct 11 00:36 WiredTiger
-rw-r----- 1 mongodb mongodb  21 Oct 11 00:36 WiredTiger.lock
-rw-r----- 1 mongodb mongodb 1255 Oct 11 12:26 WiredTiger.turtle
-rw-r----- 1 mongodb mongodb 61440 Oct 11 12:26 WiredTiger.wt
-rw-r----- 1 mongodb mongodb  4096 Oct 11 11:56 WiredTigerHS.wt
-rw-r----- 1 mongodb mongodb 20480 Oct 11 11:56 _mdb_catalog.wt
-rw-r----- 1 mongodb mongodb 20480 Oct 11 11:56 collection-0--9136015971348928900.wt
-rw-r----- 1 mongodb mongodb 36864 Oct 11 11:57 collection-2--9136015971348928900.wt
-rw-r----- 1 mongodb mongodb  4096 Oct 11 00:40 collection-4--9136015971348928900.wt
drwx-r----- 2 mongodb mongodb  4096 Oct 11 12:26 diagnostic.data
-rw-r----- 1 mongodb mongodb 20480 Oct 11 11:56 index-1--9136015971348928900.wt
-rw-r----- 1 mongodb mongodb 36864 Oct 11 11:57 index-3--9136015971348928900.wt
-rw-r----- 1 mongodb mongodb  4096 Oct 11 00:40 index-5--9136015971348928900.wt
-rw-r----- 1 mongodb mongodb  4096 Oct 11 11:57 index-6--9136015971348928900.wt
drwx-r----- 2 mongodb mongodb  4096 Oct 11 11:56 journal
-rw-r----- 1 mongodb mongodb    2 Oct 11 11:56 mongod.lock
-rw-r----- 1 mongodb mongodb 36864 Oct 11 11:58 sizeStorer.wt
-rw-r----- 1 mongodb mongodb  114 Oct 11 00:36 storage.bson
```

Figura 17: Listado de archivos binarios en el sistema

2.12.

Base de Datos	Principales características	Consideración de uso	Aspectos de seguridad relevantes
Oracle	Software multiplataforma propietario de Oracle. Es una base de datos multimodelo, implementada en C, C++ y ensamblador. Se utiliza para el procesamiento de transacciones en línea y datawarehouse.	Es un producto muy asentado en la industria, con soporte para muchas plataformas y viene avalado por Oracle. Se integra bien con otros servicios de Oracle	Oracle Database tiene una amplia sección de vulnerabilidades. Algunas vulnerabilidades destacables son en un componente del core de Oracle Database Server que da al atacante altos privilegios mediante Oracle Net [12]
MongoDB	Base de datos documental NoSQL de código abierto, multiplataforma e implementada en C++. Permite indexación de cualquier campo de un documento, replicación y fragmentación	Sistemas con un alto volumen de lecturas. Tiempo real. Manejo de documentos y de contenido	Viene sin configuración de seguridad por defecto. Hay que seleccionar de manera explícita el acceso mediante autorización y el uso de TLS/SSL para todas las conexiones
HP Vertica	Base de datos orientada a columnas diseñada para el manejo de grandes volúmenes de datos con un rendimiento de consulta elevado para datawarehouses. Permite procesamiento paralelo masivo, distintas técnicas machine learning integradas y múltiples interfaces.	Machine learning. Bajo coste. Orientada al cloud computing ya que es independiente de la plataforma y accesible en Amazon Web Service	Existen algunas vulnerabilidades importantes en algunas versiones de HP Vertica que permiten a un usuario remoto obtener privilegios [13]

Neo4j	Base de datos multiplataforma orientada a grafos compatible con ACID. Implementada en Java y con licencia dual. Implementa su propio lenguaje de consultas llamado Cypher.	Es una opción a considerar si se desea utilizar una estructura de datos que utilice estructuras de grafos para queries semánticas con nodos, aristas y propiedades o etiquetas para guardar datos con la integridad que proporcionan las bases de datos ACID.	Existen varias vulnerabilidades de Cross-Site Request Forgery en algunas versiones de Neo4J que permite a un atacante remoto secuestrar la autenticación de administración para ejecutar código arbitrario [14]
Elastic Search	Es un motor de búsqueda NoSQL distribuido para hacer búsquedas casi en tiempo real en todo tipo de documentos. Multiplataforma e implementado en Java	Tiene multitud de clientes y está fuertemente acoplado con HTTP y JSON lo cual facilita mucho su interconexión y realizar búsquedas en documentos	Existen varias vulnerabilidades relacionadas con el ELK stack (Elasticsearch, Kibana, Logstash), cabe destacar que en algunas versiones antiguas de Elasticsearch se puede bypassar la protección y ejecutar scripts en remoto [15]
MariaDB	Base de datos multiplataforma producto derivado de MySQL (base de datos relacional). Utiliza licencia GPL y está implementada en C, C++, Perl y Bash	Tiene más opciones que su predecesor en cuanto a motores de búsqueda. Proporciona estadísticas y otra meta información en nuevas tablas. Más precisión en cuanto a timestamps. Podría considerarse su uso frente a MySQL como una alternativa con más características	En algunas versiones de MariaDB existen vulnerabilidades que permiten a usuarios autenticados bypassar algunas restricciones de acceso y replicar sentencias DDL en otros nodos [16]
MS SQL	Sistema de bases de datos relacional propiedad de Microsoft que a su vez utiliza su propio lenguaje Transact-SQL para funcionar	Puede considerarse frente a otras bases de datos relacionales si se tiene un fuerte acoplamiento o dependencia con otros productos de Microsoft	Una vulnerabilidad muy conocida es muy explotable desde varios frentes, la SQL Server Remote Code Execution Vulnerability [17]

Redis	Motor de base de datos en memoria (caché) para el almacenamiento de tablas de tipo diccionario. Soporta 3 tipos de estructuras de datos (Listas, conjuntos y hashes) y antiguamente los datos no eran persistentes puesto que se guardaban en RAM.	Debido al ser un sistema que guarda los datos en RAM puede ser utilizado como base de datos auxiliar antes de utilizar otra con persistencia. Tiene multiplicidad de clientes en varios lenguajes	En algunas versiones existen vulnerabilidades que permiten hacer stack-buffer y head-buffer overflow con el comando SETRANGE [18]
PosgreSQL	Sistema de gestión de base de datos relacional implementado en C de código abierto. La principal característica es su tolerancia a la alta concurrencia lo que permite que varios procesos hagan distintas operaciones sobre una misma tabla sin bloqueos.	Puede considerarse su uso en aplicaciones con alta demanda y concurrencia sin sacrificar la integridad de los datos.	Se han encontrado vulnerabilidades recientes que permiten a un usuario ejecutar código arbitrario en el sistema. Estas vulnerabilidades están relacionadas con el programa "COPY TO/FROM PROGRAM" y con stack-buffer overflow [19]

Cuadro 1: Comparación de distintos SGBBDD

Referencias

- [1] **INSTALAR ORACLE Database 12c CON DOCKER**
Jeremy Andress
<https://medium.com/@jeremyandress/instalar-oracle-database-12c-con-docker-3a18d534c7b0>
- [2] **DockerHub**
Oracle Database Server Docker Image Documentation <https://hub.docker.com/u/pablorigort/content/sub-25333d4f-432c-4efb-8c05-49a69e19f165>
- [3] **Data Dictionary and Dynamic Performance Views**
Oracle Help Center - Database Concepts
<https://docs.oracle.com/database/121/CNCPT/datadict.htm#CNCPT1209>
- [4] **SANS ISC InfoSec Forums**
Cyber Security Awareness Month - Day 16 - Port 1521 - Oracle TNS Listener
<https://isc.sans.edu/forums/diary/Cyber+Security+Awareness+Month+Day+16+Port+1521+Oracle+TNS+Listener/7375/>
- [5] **DBA Junior**
Setup OEM Database Express
<http://www.dbajunior.com/setup-oem-database-express/>
- [6] **Oracle - Ask Tom**
about directory location of oracle database files,has it haven one parameter?
https://asktom.oracle.com/pls/apex/f?p=100:11:0:::P11_QUESTION_ID:9535318000346869801
- [7] **Database Net Services Reference**
Listener Control Utility
https://docs.oracle.com/cd/B19306_01/network.102/b14213/lsnrctl.htm
- [8] **Oracle - Help Center**
Installing Oracle Database Software and Creating a Database
https://www.oracle.com/webfolder/technetwork/tutorials/obe/db/12c/r2/2day_dba/12cr2db_ch2install/12cr2db_ch2install.html
- [9] **MongoDB Documentation**
Security
<https://docs.mongodb.com/manual/security/>
- [10] **MongoDB Documentation**
Default MongoDB Port
<https://docs.mongodb.com/manual/reference/default-mongodb-port/>
- [11] **MongoDB Documentation**
Journaling
<https://docs.mongodb.com/manual/core/journaling/>
- [12] **CVE Details**
Oracle Database Security Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-18751/version_id-221169/Oracle-Database-12.2.0.1.html

- [13] **CVE Details**
HP Vertica Security Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-10/product_id-32574/HP-Vertica.html
- [14] **CVE Details**
Neo4J Security Vulnerabilities [CVE-2013-7259]
<https://www.cvedetails.com/cve/CVE-2013-7259/>
- [15] **CVE Details**
Elasticsearch Security Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-13554/Elasticsearch.html
- [16] **CVE Details**
MariaDB 10.2.0 Security Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-12010/product_id-22503/version_id-207752/Mariadb-Mariadb-10.2.0.html
- [17] **CVE Details**
Microsoft SQL Server Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-251/Microsoft-Sql-Server.html
- [18] **CVE Details**
Redis Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-18560/product_id-47087/version_id-307209/Redislabs-Redis-5.0.3.html
- [19] **CVE Details**
Postgresql Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-336/product_id-575/year-2019/ope-1/Postgresql-Postgresql.html