

Seguridad en Bases de Datos

UNIDAD III

Cifrado en bases de datos de Oracle

La mayoría de los datos relacionales; son los objetivos ideales para los **hackers** que buscan objetivos de alto **valor para el robo de datos**. El riesgo de una sola base de datos de Oracle Database puede resultar en decenas de millones de registros violados y un costo de varios millones de dólares.

— — —



¿Cómo proteger los datos?

Cifrado en bases de datos de Oracle

¿Cómo proteger los datos?

Existen controles de seguridad preventivos y de detección:

- Cifrado de datos transparentes
- La gestión de claves de cifrado
- El control de acceso multifactor y de usuarios autorizados
- La detección y clasificación de datos
- El bloqueo y supervisión de la actividad en bases de datos

-
- La creación de informes y auditorías consolidados
 - El enmascaramiento de datos.

Con los SGBD, puede desplegar soluciones de seguridad de datos fiables que no requieren cambios en las aplicaciones existentes y que permiten ahorrar tiempo y dinero.

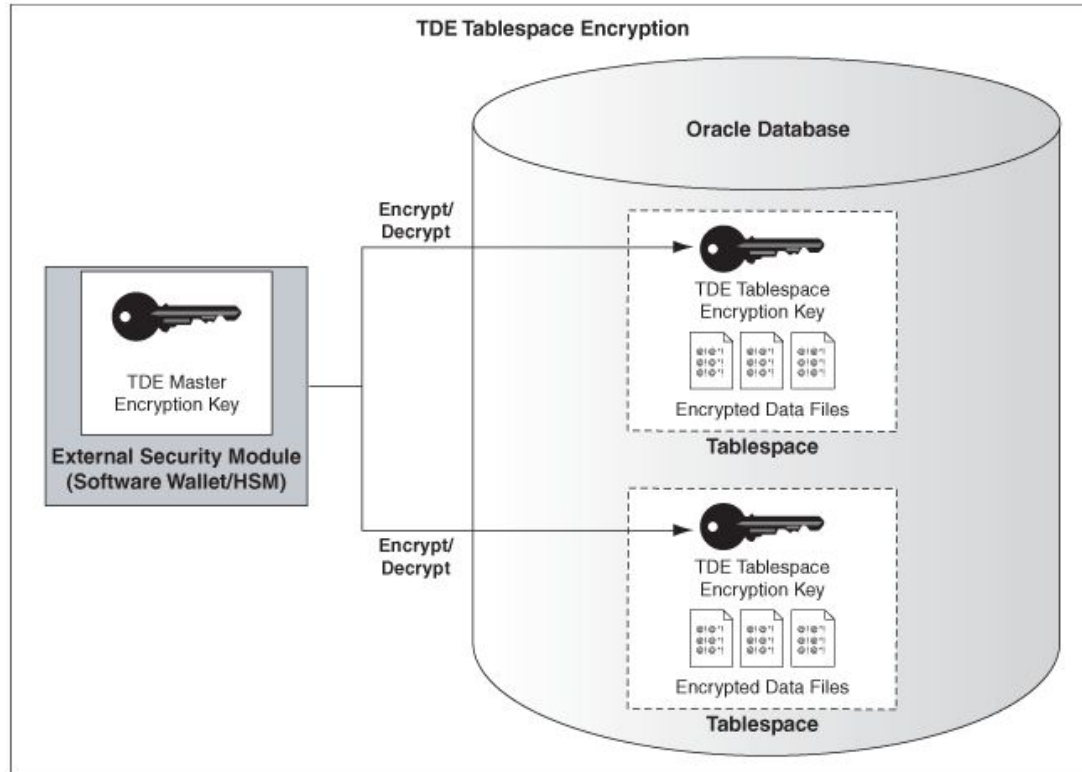
Cifrado en bases de datos de Oracle

El cifrado transparente de datos:

- Evita que los atacantes potenciales omitan la base de datos y lean información confidencial directamente desde el almacenamiento al aplicar el cifrado de datos.
- **Dos modos de cifrado:**
 - **Cifrado de espacios de tabla (TDE):** Se utiliza para cifrar tablas de aplicaciones completas
 - **Cifrado de columnas:** cifra elementos de datos individuales que contienen información confidencial.

Modos de cifrado

Cifrado de espacios de tabla

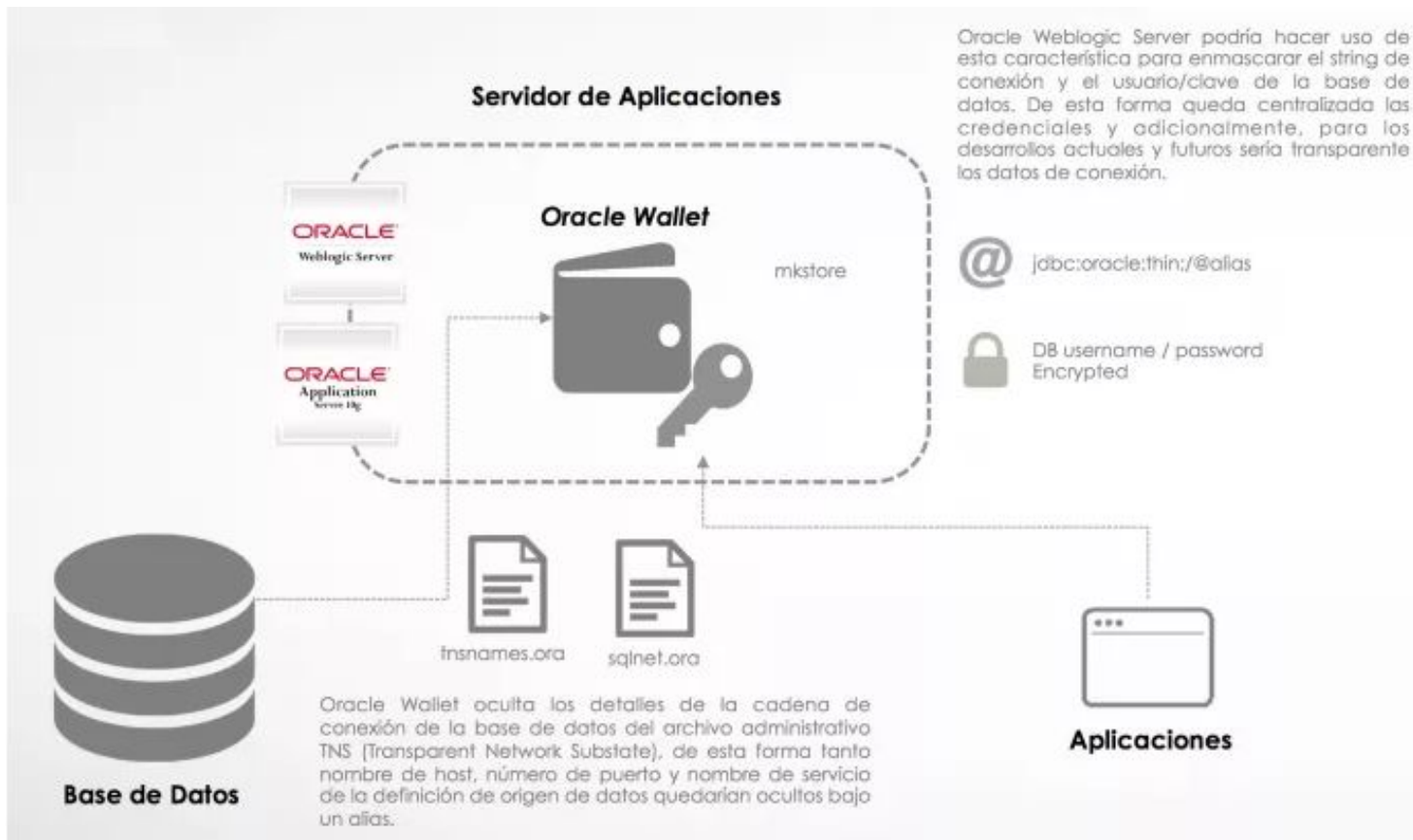


El cifrado de espacios de tabla **TDE** utiliza la arquitectura de **dos niveles basada** en claves para **cifrar (y descifrar)** de manera transparente los espacios de tabla.

La clave maestra de TDE se almacena en un módulo de seguridad externo (Oracle Wallet)

Modos de cifrado

¿Qué es y cómo usar Oracle Wallet?



Modos de cifrado

¿Qué es y cómo usar Oracle Wallet?

Oracle Wallet es un método para administrar credenciales de bases de datos en varios dominios y en las capas de orígenes de datos de los servidores de aplicaciones.

Oracle Wallet permite actualizar las credenciales de base de datos actualizando la “cartera” en lugar de tener que cambiar todas las definiciones de los orígenes de datos individualmente. Esto se logra utilizando una cadena de conexión de base de datos en la definición de origen de datos que posteriormente se resuelve mediante una entrada en la “cartera”.

El Wallet es un directorio dentro del servidor donde están escritas las contraseñas (en forma encriptada) por el **comando mkstore**. Paso seguido se le indica a la base de datos dónde encontrar el Wallet configurando parámetros específicos en el archivo **sqlnet.ora** y recuperar/usar una contraseña almacenada haciendo referencia a un alias TNS configurado en su archivo **tnsnames.ora**. Por lo que no hay servicios que debas iniciar o detener, ni debes instalar nada en particular.

Modos de cifrado

Cifrar

Peticiónes de Datos SQL

Propietario: C##ARACELI

Nombre: T1

Algoritmo de Cifrado: AES192

Sin Salt: ☐

Cifrar Columna Seleccionada

Ayuda Aplicar Cancelar

Para comenzar a usar TDE, el administrador de seguridad debe crear una cartera y establecer una clave maestra.

- AES256: AES (tamaño de clave de 256 bits)
- AES192: AES (tamaño de clave de 192 bits)
- 3DES168: Triple-DES de 3 teclas (tamaño de clave efectivo de 168 bits)
- AES128: AES (tamaño de clave de 128 bits)
- 3DES112: Triple-DES de 2 teclas (tamaño de clave efectivo de 112 bits)

Seguridad en la interacción Aplicación

Con esto podemos resumir los beneficios de **Oracle Wallet** de la siguiente manera:



Seguridad en la interacción Aplicación



Gestión de privilegios de acceso a BD

The screenshot displays the MySQL Server Administration interface. The left sidebar contains a 'MANAGEMENT' section with 'Users and Privileges' highlighted. The main area shows the 'localhost' connection details, including the MySQL logo, host, socket, port, version, and configuration file. The 'Available Server Features' section lists various settings like Performance Schema, Thread Pool, and SSL Availability. The 'Server Directories' section is partially visible at the bottom. The right sidebar shows a 'Server Status' overview with metrics like CPU Load (52%), Connections (4), Traffic (28.64 KB/s), and InnoDB Buffer Usage (51.2%).

Navigation: SQL File 10*, SQL File 13*, SQL File 14*, SQL File 5*, SQL File 6*, SQL File 7*, SQL File 8*, Administration - Server Status x

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges**
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

Administration Schemas

Information

No object selected

Connection Name: localhost

MySQL Server

Host: Datic-Araceli
Socket: MySQL
Port: 3306
Version: 8.0.15 (MySQL Community Server - GPL)
Compiled For: Win64 (x86_64)
Configuration File: C:\ProgramData\MySQL\MySQL Server 5.5\my.ini
Running Since: Fri Jul 26 09:06:40 2019 (2 days 9:41)

Available Server Features

Performance Schema:	<input checked="" type="radio"/> On	Windows Authentication:	<input type="radio"/> Off
Thread Pool:	<input type="radio"/> n/a	Password Validation:	<input type="radio"/> n/a
Memcached Plugin:	<input type="radio"/> n/a	Audit Log:	<input type="radio"/> n/a
Semisync Replication Plugin:	<input type="radio"/> n/a	Firewall:	<input type="radio"/> n/a
SSL Availability:	<input checked="" type="radio"/> On	Firewall Trace:	<input type="radio"/> n/a

Server Directories

Base Directory: C:\Program Files\MySQL\MySQL Server 8.0\

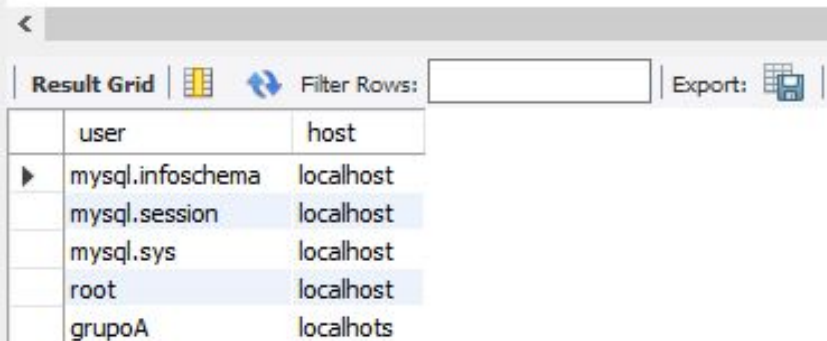
Server Status Overview:

- Server Status: Running
- CPU/Load: 52%
- Connections: 4
- Traffic: 28.64 KB/s
- Key Efficiency: 0.0%
- Selects per Second: 0
- InnoDB Buffer Usage: 51.2%
- InnoDB Reads per Second: 0
- InnoDB Writes per Second: 0

Gestión de privilegios de acceso a BD

En MySQL: Crear usuario

```
1 • create user grupoA@'localhost';  
2 • use mysql;  
3 • select user from user;  
4 • select user, host from user;
```



The screenshot shows a MySQL client interface with a 'Result Grid' tab selected. The grid displays the output of the SQL command 'select user, host from user;'. The table has two columns: 'user' and 'host'. The rows listed are: 'mysql.infoschema' (localhost), 'mysql.session' (localhost), 'mysql.sys' (localhost), 'root' (localhost), and 'grupoA' (localhots). The 'grupoA' row is highlighted in blue.

	user	host
▶	mysql.infoschema	localhost
	mysql.session	localhost
	mysql.sys	localhost
	root	localhost
	grupoA	localhots

Gestión de privilegios de acceso a BD

En MySql: Crear usuario y privilegio (grant)

The screenshot shows the MySQL Workbench Administration - Users and Privileges window. The left sidebar contains a 'MANAGEMENT' section with 'Users and Privileges' highlighted. The main area shows a table of 'User Accounts' with columns 'User' and 'Host'. The 'Add Account' button is highlighted with a blue box.

User	Host
grupoA	localhost
mysql.infoschema	localhost
mysql.session	localhost
mysql.sys	localhost
root	localhost

Buttons: Add Account, Delete, Refresh

Privilegios en la base de datos

¿Qué son los privilegios?

Los privilegios son el derecho a ejecutar sentencias SQL en particular. El DBA (administrador de la base de datos) es un usuario de alto nivel con la capacidad de crear usuarios y de otorgarles acceso a la base de datos y a sus objetos

Privilegios en la base de datos

La base de datos tiene **dos** tipos de privilegios:

De sistema: estos privilegios le permiten al usuario realizar acciones específicas sobre la base de datos.

De objetos: estos privilegios le permiten al usuario acceder y manipular objetos específicos.

Privilegios en la base de datos

Creación de un usuario

Para crear el usuario, el DBA ejecuta la sentencia **CREATE USER**.

Sintaxis:

— — —

```
CREATE USER user  
IDENTIFIED BY password;
```

```
CREATE USER jazmin  
IDENTIFIED BY adm1n15tr4d0r;
```


Privilegios en la base de datos

Privilegios de sistema

Sintaxis.

```
GRANT privilege [, privilege...]  
TO user [, user| role, PUBLIC...];  
— — —
```

```
GRANT create session, create table,  
create sequence, create view  
TO administrador;
```

- **privilege** es el privilegio del sistema que se va a otorgar.
- user |role|**PUBLIC** es el nombre del usuario, el nombre del rol o, en el caso de **PUBLIC**, designa que el privilegio se otorga a todos los usuarios.

Privilegios en la base de datos

Privilegios de sistema

<i>Privilegio del Sistema.</i>	<i>Operaciones Autorizadas</i>
CREATE USER	La persona a la que se otorga el privilegio puede crear otros usuarios de Oracle.
DROP USER	La persona a la que se otorga el privilegio puede borrar otro usuario.
DROP ANY TABLE	La persona a la que se otorga el privilegio puede borrar una tabla de cualquier esquema.
BACKUP ANY TABLE	La persona a la que se otorga el privilegio puede realizar copias de seguridad de cualquier esquema con la utilidad de exportación.
SELECT ANY TABLE	La persona a la que se otorga el privilegio puede consultar tablas, vistas o instantáneas en cualquier esquema.
CREATE ANY TABLE	La persona a la que se otorga el privilegio puede crear tablas en cualquier esquema.

Privilegios en la base de datos

Privilegios de sistema

<i>Privilegio del Sistema</i>	<i>Operaciones Autorizadas</i>
CREATE SESSION	Conectarse a la base de datos
CREATE TABLE	Crear tablas en el esquema del usuario
CREATE SEQUENCE	Crear una secuencia en el esquema del usuario
CREATE VIEW	Crear una vista en el esquema del usuario
CREATE PROCEDURE	Crear un procedimiento, una función o un paquete en el esquema del usuario

Privilegios en la base de datos

Privilegios de objetos

Sintaxis.

```
GRANT object_priv|all| [(columns)]  
ON object  
TO {user|role|PUBLIC}  
[WITH GRANT OPTION];
```

object_priv es un privilegio de objeto que se va a otorgar.

- *ALL* especifica todos los privilegios de objeto.
- *columns* especifica la columna de una tabla o de una vista en la que se otorgan los privilegios.
- *ON object* es el objeto en el que se otorgan privilegios.
- *TO* identifica a quién se otorga el privilegio.
- *PUBLIC* otorga privilegios de objeto a todos los usuarios.
- ***WITH GRANT OPTION*** permite a la persona a la que se otorga el privilegio otorgar privilegios de objeto a otros usuarios y roles.

Privilegios en la base de datos

Privilegios de objetos

Sintaxis.

```
GRANT all  
ON hr.departments  
TO administrador;
```

El usuario administrador puede consultar, insertar, actualizar y eliminar registros en la tabla departments del esquema hr.

Privilegios en la base de datos

Revocación de privilegios de objetos

Sintaxis.

```
REVOKE {privilege [, privilege...]|ALL}  
ON object  
FROM {user[, user...]|role|PUBLIC}  
[CASCADE CONSTRAINTS];
```

CASCADE es necesario para eliminar cualquier restricción de integridad referencial realizada en el objeto CONSTRAINTS mediante el privilegio REFERENCES.