

CURSOS  
INTERSEMESTRALES



PROTECO

# Administración de bases de datos

SQLII

# IDENTIFICACIÓN DE LA VERSIÓN DE LA BASE DE DATOS

A nivel general, cualquier base de datos hace uso de una serie de caracteres y/o dígitos para especificar la versión de la base de datos a emplear.

Para el caso de Oracle se emplean 5 dígitos.

Se definen 2 tipos de versiones:

- version
- version\_full (Actualización de la versión mayor de forma trimestral).



# Ejemplo

18	0	0	0	0
Major Release.	Release Update Version.	Release update Revision version.	version Increment.	Reservado para uso futuro.
Formada por los 2 últimos dígitos del año en el que se libera por primera vez.	Numero de actualización. Oracle produce actualizaciones trimestrales.	Representa el número de revisión de la actualización trimestral.	Empleado para actualizaciones en versiones futuras	



# CUENTAS DE USUARIO DE ADMINISTRACIÓN Y PRIVILEGIOS.

Dependiendo el sistema operativo, una base de datos puede requerir de las siguientes cuentas de usuarios para poder ser administrada:

- Cuenta de usuario administrador a nivel del sistema operativo. Permite administrar el control de acceso a los archivos que integran el software de la base de datos (depende del sistema operativo). Para el caso de sistemas Unix/Linux se requiere la existencia del usuario oracle.
- Cuentas de usuarios administradores a nivel de la base de datos.



# Cuentas de usuario a nivel de la base de datos.

Nombre del usuario	Descripción
sys	Cuenta con todos los privilegios asignados. Todas las tablas y vistas del diccionario de datos son almacenadas en el esquema SYS. Usuarios no modifican estas vistas y tablas, y <u>tampoco debe crear nuevas</u> .
system	Se le asigna el rol DBA. Se emplea para crear tablas y vistas adicionales que muestran información de administración empleadas por herramientas y funcionalidades adicionales que ofrece la BD. De forma similar, no se debe emplear este esquema para crear nuevas tablas.
sysbackup	Facilita el manejo y administración de respaldos empleando SQL *Plus o RMAN (Recovery Manager).
sysdg	Se encarga de realizar operaciones con funcionalidades de "Data Guard". Data Guard ofrece la implementación de requerimientos como Alta disponibilidad, protección de datos, recuperación ante desastres, etc., a través de operaciones de creación, mantenimiento y monitoreo de BDs.
syskm	Empleado para realizar y ejecutar funcionalidades asociadas con Cifrado de datos, generación de KeyStores, etc.
sysrac	Empleado para realizar operaciones de administración en ambientes clusterizados a través de Oracle RAC. Conexión entre nodos del clúster, etc.



# Privilegios de administración.

Privilegio	Operaciones principales permitidas.
sysdba	<code>startup, shutdown</code> <code>alter database: open, mount, back up, change character set</code> <code>create database</code> <code>drop database</code> <code>create spfile</code> <code>alter database archivelog</code> <code>alter database recover</code> Permite realiza la mayoría de las operaciones incluida la posibilidad de ver los datos de los usuarios, representa el privilegio con el mayor poder.
sysoper	<code>startup, shutdown</code> <code>create spfile</code> <code>alter database: open, mount, back up</code> <code>alter database archivelog</code> <code>alter database recover</code> (solo recuperación completa). No puede ver los datos de los usuarios.
sysbackup	La lista de operaciones que puede realizar este privilegio está definida a través del rol sysbackup
sysdg	La lista de operaciones que puede realizar este privilegio está definida a través del rol sysdg
syskm	La lista de operaciones que puede realizar este privilegio está definida a través del rol syskm
sysrac	La lista de operaciones que puede realizar este privilegio está definida a través del rol sysrac





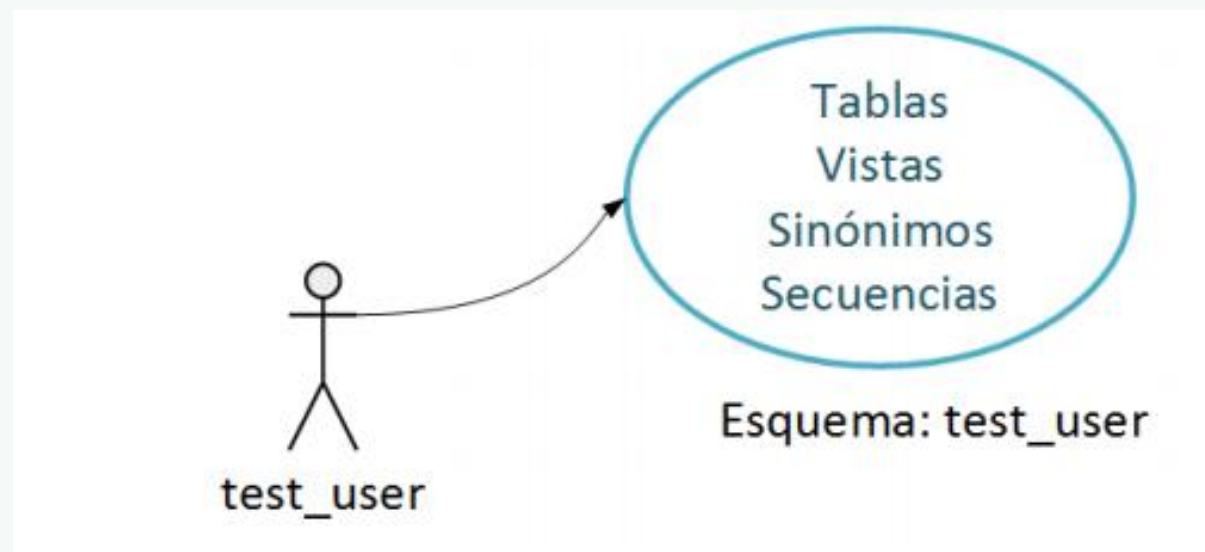
Para hacer uso de los privilegios de administración se requiere realizar lo siguiente:

- El usuario debe tener asignado alguno de estos privilegios, por ejemplo, el usuario SYS se los ha asignado anteriormente.
- Para hacer uso de dicho privilegio, el usuario debe conectarse a la BD indicando el privilegio de administración con el que desea conectarse.



Cuando un usuario se conecta a la BD sin hacer uso de un privilegio de administración ocurre lo siguiente:

- Al entrar a sesión, el usuario tiene asociado a un esquema cuyo nombre coincide con su nombre de usuario. Por ejemplo, el usuario `test_user` tiene un esquema llamado `test_user`.







Cuando un usuario se conecta a la BD empleando un privilegio de administración, la regla anterior cambia

- Al conectarse como sysdba, el esquema asignado es sys.
- Al conectarse como sysoper, el esquema asignado es public.
- Al conectarse como sysbackup, sysdg, y sysrac el esquema asignado es sys.
- Al conectarse como syskm, el esquema asignado es syskm





Otra característica del uso de los privilegios de administración es que el usuario también cambia:

- Al conectarse como sysdba, el usuario asignado es sys.
- Al conectarse como sysoper, el usuario asignado es public.
- Al conectarse como sysbackup, sysdg, syskm y sysrac el usuario asignado es sysbackup, sysdg, syskm y sysrac respectivamente



# Métodos de autenticación para usuarios con privilegios de administración

- A través del diccionario de datos (cuando la BD está iniciada).
- A través de un archivo de passwords (útil cuando la BD no está iniciada).
- A través del sistema operativo.
- Empleando un servicio de autenticación externo (directory-based authentication service), por ejemplo, Oracle Internet Directory.



# Autenticación vía sistema operativo

Para realizar la autenticación vía sistema operativo, el usuario debe pertenecer a un grupo especial.

Nombre del grupo del sistema operativo	Privilegio de administración.
dba	sysdba
oper	sysoper
backupdba	sysbackup
dgdba	sysdg
syskm	kmdba
sysrac	racdba

*connect / as sysdba*

*connect / as sysoper*

# Autenticación empleando archivo de passwords

- El archivo de passwords se crea durante el proceso de creación de la base de datos empleando dbca (Database Configuration Assistant).
- El archivo debe contar con un nombre y ubicación con base a las siguientes reglas:
  - En Unix/Linux el nombre debe ser orapwORACLE\_SID. ORACLE\_SID corresponde al valor de la variable de entorno revisada anteriormente.
  - Debe ubicarse en \$ORACLE\_BASE/dbs para casos donde se ha decidido definir al directorio ORACLE\_HOME como read only, (funcionalidad agregada en 18c). De lo contrario se ubica en \$ORACLE\_HOME/dbs.
- Para hacer uso del archivo de passwords, un usuario con privilegios de administración podrá autenticarse en SQL \*Plus aun con la base de datos detenida empleando las siguientes instrucciones:



```
jorge@lap-red-mint ~ $ su -l oracle
Password:
oracle@lap-red-mint:~$ sqlplus /nolog
```

```
SQL*Plus: Release 18.0.0.0.0 - Production on Sat Jul 20 13:25:04 2019
Version 18.3.0.0.0
```

```
Copyright (c) 1982, 2018, Oracle. All rights reserved.
```

```
-SQL> --¿Qué sucederá al ejecutar la siguiente instrucción?
```

```
-SQL> connect usr_noexiste as sysdba
```

Una forma de alimentar el archivo de password es a través de SQL\*Plus. El archivo se modifica automáticamente cuando se le asigna un privilegio de administración a algún usuario



# EL COMANDO STARTUP

En una operación normal de inicio, el comando startup, inicia la instancia, monta y posteriormente, abre una base de datos. Un usuario puede acceder a la BD una vez que esta se encuentra abierta. Existen varios mecanismos para levantar una instancia:

- A través de SQL \*Plus
- A través de Oracle restart
- A través del uso de Recovery Manager.
- Empleando Oracle Enterprise Manager Cloud Control



## Modos de inicio

Modo	Descripción
<code>startup nomount</code>	<p>Inicia la instancia sin montar la BD:</p> <ul style="list-style-type: none"><li>• Se crean todas las áreas de memoria</li><li>• Los procesos de background son creados</li><li>• Se ubica al archivo de parámetros considerando el siguiente orden y nombres de archivos: Orden 1: <code>spfileSID.ora</code> Orden 2: <code>spfile.ora</code> Orden 3: <code>initSID.ora</code> En caso de no encontrar alguno de estos archivos, se produce error.</li></ul> <ul style="list-style-type: none"><li>• En este modo no es posible acceder a la Base de Datos, inclusive puede no existir.</li><li>• Se emplea generalmente para:<ul style="list-style-type: none"><li>○ Crear una nueva base de datos</li><li>○ Re-crear archivos de control.</li></ul></li><li>• En este modo se utilizan únicamente 2 archivos: <i>archivo de parámetros</i> y el <i>alert log</i>.</li></ul>







startup mount

Inicia la instancia, monta la BD:

- Ubica y lee el contenido del archivo de control y lo lee. Su ubicación lo obtiene del parámetro `control_files`.
- Si existen varias copias estos deben ser idénticos, todos disponibles.
- En este estado la BD permanece cerrada, no se tiene acceso aun a ella.
- El DBA puede realizar algunas tareas administrativas.

El siguiente procedimiento puede ser útil cuando se desea regenerar un archivo de control:

1. `shutdown immediate;`
  2. `alter database backup controlfile to trace as '$ORACLE_HOME/dbs/control_new.sql';`
  3. La instrucción anterior permite crear un script SQL que al ser ejecutado generará o recuperará el archivo de control.
  4. Modificar el script en caso de ser necesario.
  5. Ejecutar el script: `@$ORACLE_HOME/dbs/control_new.sql`
  6. `alter database mount`
  7. `alter databse open`
- Se leen las ubicaciones y nombres de los data files y los online redo logs.  
Nota: Solo se obtienen las ubicaciones. Los archivos no se validan aun.  
Esto se hace en la siguiente etapa.



startup open	<p>Inicial la instancia, monta la BD y se abre:</p> <ul style="list-style-type: none"> <li>• A partir de las ubicaciones y nombres de los data files y online redo logs, se lee su contenido y se revisa estos archivos están sincronizados. Es decir, todas las transacciones fueron sincronizadas. Si esto ocurre, se procede a abrir la BD. De lo contrario inicia el proceso de recuperación (se revisará más adelante).</li> <li>• La BD puede ser accedida a partir de este momento.</li> </ul>
startup force	<ul style="list-style-type: none"> <li>• Realiza un inicio forzado posterior a la ocurrencia de algún problema al detener o iniciar.</li> </ul>
startup open recover	<ul style="list-style-type: none"> <li>• Abre la BD y procede inmediatamente a realizar una posible recuperación de la base de datos: <i>media recovery</i>.</li> </ul>



# Problemas que pueden ocurrir

El inicio normal de la instancia y apertura de la BD puede verse afectada por problemas comunes como son:

- Archivo de control dañado o no disponible
- Si alguno de los archivos especificados en el archivo de control no están disponibles, la BD no se podrá montar.



# Modificando el modo de inicio de la instancia.

Comando	Descripción
<code>alter database mount</code>	Cambia el estado actual de la instancia a modo mount
<code>alter database open</code>	Cambia el estado actual de la instancia a modo open
<code>alter database open read only</code>	<ul style="list-style-type: none"><li>• Permite realizar consultas a la base de datos pero evita cualquier cambio o modificación a los Online Redo Logs files, o a los data files.</li><li>• Existe un escenario donde si se pueden modificar estos archivos: Recovery.</li></ul>
<code>alter database open read write</code>	<ul style="list-style-type: none"><li>• Es el valor por default, equivalente a la instrucción <code>alter database open</code>.</li></ul>



# SHUTDOWN

Comando	Descripción
<code>shutdown normal</code>	<p>Representa la opción por default.</p> <ul style="list-style-type: none"><li>• No más conexiones se permiten</li><li>• Si existen usuarios actualmente conectados, la instancia espera a que cierren su sesión para detener la instancia.</li><li>• Se realiza el cierre ordenado de la BD y sincronización, por lo que no se requerirá proceso de recuperación.</li></ul>
<code>shutdown immediate</code>	<ul style="list-style-type: none"><li>• No más conexiones se permiten</li><li>• Para las sesiones actuales no nuevas transacciones son permitidas.</li><li>• Para las transacciones no concluidas se aplica <code>rollback</code> y se concluyen.</li><li>• No espera a que usuarios conectados se desconecten. Las sesiones se cierran inmediatamente.</li><li>• Se realiza el cierre ordenado de la BD y sincronización, por lo que no se requerirá proceso de recuperación.</li></ul>
<code>shutdown transactional</code>	<ul style="list-style-type: none"><li>• No más conexiones se permiten</li><li>• Para las sesiones actuales no nuevas transacciones son permitidas.</li><li>• A diferencia del modo anterior, el manejador espera a que transacciones en curso terminen.</li><li>• Si al término de todas las transacciones aún existen usuarios conectados, cierra sus sesiones y los desconecta.</li><li>• Se realiza el cierre ordenado de la BD y sincronización, por lo que no se requerirá proceso de recuperación.</li></ul>





Shutdown abort	<p>Cierra la base de datos de forma instantánea.</p> <ul style="list-style-type: none"><li>• Esta opción debería emplearse únicamente en casos de emergencia, ante la inminente ocurrencia de un problema o falla.</li><li>• Este modo realiza las mismas acciones que <code>shutdown immediate</code>.</li><li>• La diferencia es que archivos y buffers no son sincronizados por lo que el próximo inicio seguramente va a requerir proceso de <u>recuperación</u>.</li></ul>
----------------	---

- Esta opción debería emplearse únicamente en casos de emergencia, ante la inminente ocurrencia de un problema o falla.
- Este modo realiza las mismas acciones que `shutdown immediate`.
- La diferencia es que archivos y buffers no son sincronizados por lo que el próximo inicio seguramente va a requerir proceso de recuperación.



# INACTIVAR UNA BASE DE DATOS

- Inactivar una base de datos impide a usuarios que no cuenten con privilegios de administración
- conectarse a la instancia.
- Únicamente usuarios con privilegios de administración pueden crear sesiones.
- Sesiones actualmente conectadas al momento de inactivar la BD se les permite continuar siempre y cuando estén activas (ejecutando transacciones, bloqueando recursos, etc.).



- Sesiones inactivas no se desconectan, pero si intentan ejecutar sentencias, la sesión será puesta en modo de espera hasta que la BD sea activada nuevamente
- El status de inactividad de la instancia se puede consultar en

*v\$instance empleando el atributo  
active\_state.*





# SUSPENDER UNA BASE DE DATOS

- Cuando una base de datos se suspende a través de la sentencia alter system suspend, toda la actividad de lecturas y escrituras hacia los data files y archivos de control se detiene.
- Esta característica permite por ejemplo, realizar un respaldo de la base de datos sin posibles interferencias o cambios realizados a estos archivos durante el proceso de backup

status from v\$instance;



- Al momento de ejecutar la sentencia, todas las operaciones I/O existentes se les permite terminar, pero nuevas peticiones para realizar operaciones I/O son detenidas y se les asigna el status `queued`
- Para suspender una base de datos se emplea:  
*alter system suspend;*
- Para resumir o terminar la suspensión se emplea:  
*alter system resume;*
- La siguiente sentencia se emplea para verificar si una instancia está suspendida.  
*select database\_status from v\$instance;*

