UNIVERSIDAD PRIVADA DE TACNA

INGENIERIA DE SISTEMAS

TITULO:

INFORME LABORATORIO 06

CURSO:

BASE DE DATOS II

DOCENTE:

ING. Patrick Cuadros Quiroga

Integrantes:

Condori Gutierrez, Flor de Maria	(2015053227)
Salamanca Contreras, Fiorella Rosmery	(2015053237)
Escalante Maron, Nelia	(2014049551)

Índice

1. Respuesta al ejecutar los siguientes comandos

¿Qué sucede al ejecutar los siguientes comandos?

- STARTUP OPEN

  Una base de datos Oracle puede estar en uno de estos cuatro estados: OPEN: La base de datos está completamente funcional. Para ello se abren los archivos de datos y los Redo Log y se comprueba la consistencia de los datos.

  Este es el valor por defecto para arrancar, montar y abrir una base datos.

  Abrir la base de datos incluyendo las siguientes tareas:

  * Apertura de los archivos de datos en línea.
  * Apertura de los archivos de registro de rehacer en línea.

- STARTUP MOUNT

  Una base de datos Oracle puede estar en uno de estos cuatro estados: MOUNT: Al estado anterior se añade la lectura de los archivos de control que permiten determinar cómo se ha de preparar la instancia. Se buscan los archivos de datos y los Redo Log, comprobando su existencia en las rutas marcadas por el archivo de control.

  En este estado podemos conectar (como administradores) y realizar tareas como:

  * Cambio del nombre de los archivos de datos.
  * Activar el modo ARCHIVELOG.
  * Recuperación de la base de datos
  * En definitiva, tareas sobre los archivos de la base de datos ya que aun no se han abierto sus datos.

  Arrancamos la base de datos montada, normalmente se usa en modo para tareas de mantenimiento.

– STARTUP NOMOUNT

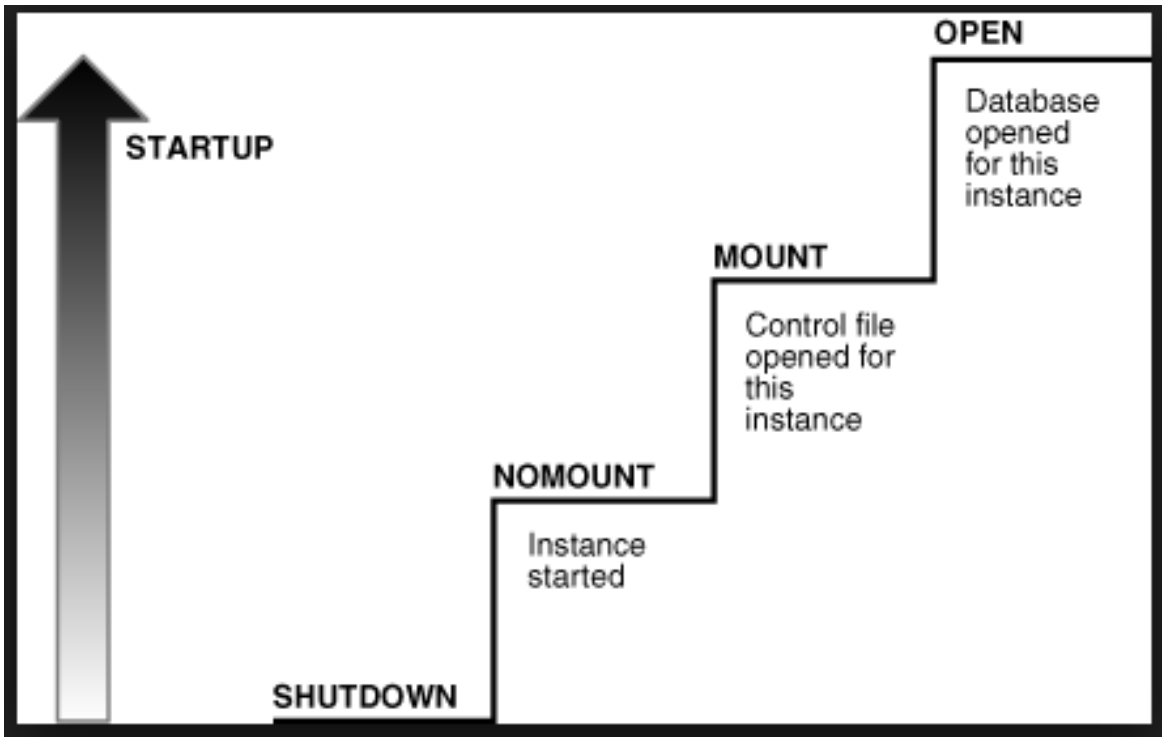
Una base de datos Oracle puede estar en uno de estos cuatro estados:

NOMOUNT: La instancia de base de datos está latente en memoria, con los procesos comunes funcionando. Se abre el archivo de parámetros, se asigna en memoria el espacio para la SGA, se lanzan los procesos en segundo plano, se abren los archivos de traza y alerta.

Arrancamos la base de datos (instancia) pero sin montarla, se suele usar la fase de creación de una base de datos.

Una instancia se inicia normalmente solo en modo Nomount durante:

* Creación de base de datos
* Recreación de archivos de control.
* Ciertos escenarios de copia de seguridad y recuperación.



– STARTUP FORCE

Arranque con un fichero de parámetros distinto al habitual o localizado en una situación diferente a donde se encuentra por defecto.

Si la base de datos está abierta, FORCE apaga la base de datos con una SHUTDOWN ABORT declaración antes de volver a abrirla. Si la base de datos está cerrada, entonces FORCE abre la base de datos.

Puede usar la opción de inicio de STARTUP FORCE si tiene dificultades para iniciar la

base de datos de una manera normal. Por ejemplo, si un servidor de base de datos perdió energía y la base de datos se detuvo bruscamente, puede dejar la base de datos en un estado en el que sea necesario un inicio de STARTUP FORCE.

Este tipo de inicio normalmente no debería ser requerido, pero puede usarse si un inicio normal no funciona. STARTUP FORCE realiza un aborto de apagado y luego reinicia la base de datos.

– STARTUP RESTRICT

Es un modo especial de trabajo en el que la base de datos está abierta, pero solo se permite el acceso a usuarios con permiso RESTRICTED (lo poseen los administradores) para hacer tareas especiales de administración. Uso:

STARTUP RESTRICTED

Si la instancia ya estaba abierta es:

ALTER SYSTEM ENABLE RESTRICTED SESSION;

Y si lo que queremos es desactivar el modo restringido para pasar a modo normal:

ALTER SYSTEM DISABLE RESTRICTED SESSION;

Arrancamos la base de datos en modo restringido, solo usuario que tengan privilegios de CREATE SESSION y RESTRICTED SESSION podrán conectarse.

La opción STARTUP RESTRICT inicia la base de datos y la coloca en modo ABIERTO, pero da acceso solo a los usuarios que tienen el privilegio RESTRICTED SESSION. Es posible que desee abrir una base de datos utilizando la opción RESTRINGIDA cuando desee realizar el mantenimiento de la base de datos mientras esté abierta, pero asegúrese de que los usuarios no puedan conectarse y realizar trabajos en la base de datos.

Es posible que también desee abrir la base de datos utilizando la opción RESTRINGIDA para realizar exportaciones o importaciones de la base de datos y garantizar que ningún usuario acceda al sistema durante estas actividades. Una vez que haya terminado con su trabajo, puede deshabilitar la sesión restringida, ALTERAR LA SESIÓN RESTRINGIDA DEL SISTEMA, para que todos puedan conectarse a la base de datos.

– STARTUP RECOVER

Especifica que la recuperación de medios se debe realizar, si es necesario, antes de iniciar la instancia. STARTUP RECOVER tiene el mismo efecto que emitir el comando RECOVER DATABASE e iniciar una instancia. Solo la recuperación completa es posible con la opción RECUPERACIÓN.

La recuperación continúa, si es necesario, como si AUTORECOVERY estuviera en ON,

independientemente de si AUTORECOVERY está habilitado o no. Si no se encuentra un archivo de registro de rehacer en la ubicación esperada, la recuperación continúa como si AUTORECOVERY estuviera deshabilitado, al indicarle la ubicación sugerida y el nombre de los archivos de registro posteriores que deben aplicarse.

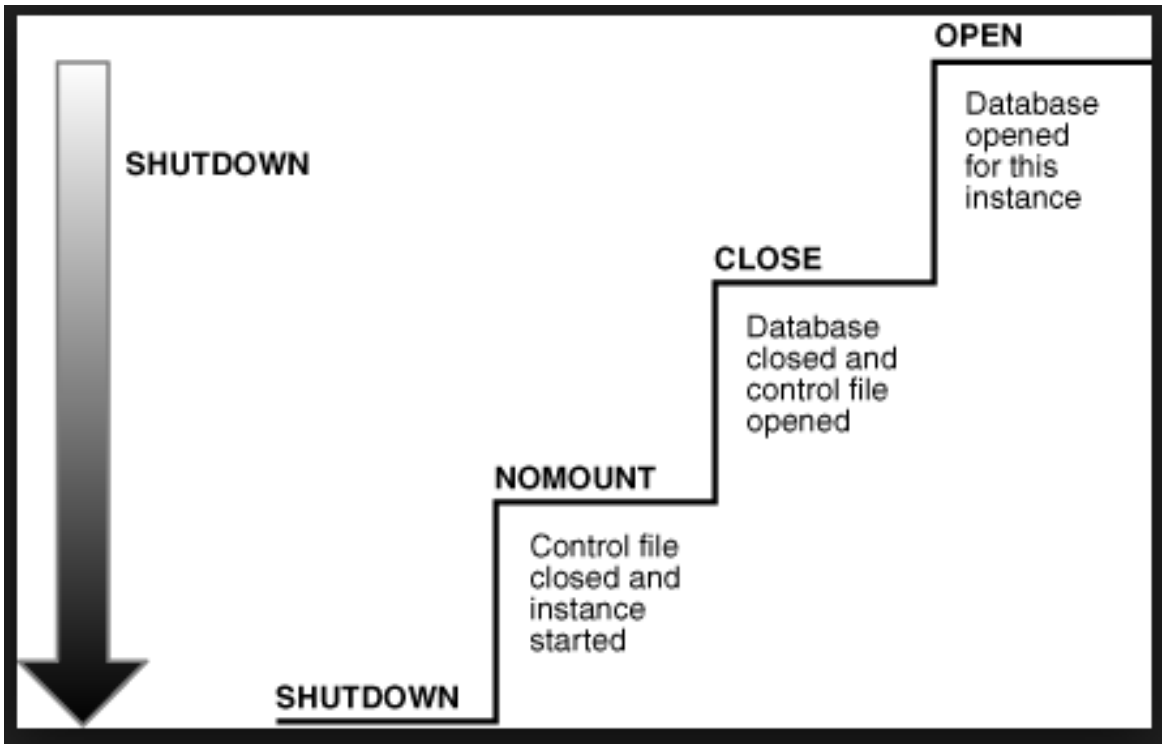
– SHUTDOWN NORMAL

Una instancia cuando es arrancada, hasta estar disponible atraviesa todos los estados anteriores.
El comando de apagado de la instancia es SHUTDOWN, su sintaxis:

NORMAL: Modo en el que no se admiten más conexiones a la base de datos, pero las actuales se mantienen. Cuando se cierre la última sesión, la base de datos pasará a estar cerrada (SHUTDOWN), pero, hasta entonces, seguirá abierta. Al cerrar se fuerza un checkpoint y se graban todos los datos del búfer, además de cerrarse los archivos.

Caracteristicas:

* Espera a que los usuarios conectados actualmente finalicen TODAS las operaciones.
* Evita nuevas conexiones. Los usuarios que intentan conectarse reciben el mensaje "Shutdown in progress".
* Cierra y desmonta la B.D. Cierra la SGA para los procesos background.
* No necesita recuperacion al arrancar la base de datos.



2. Privilegios de sistema (DDL) utilizados del script proporcionado lab_02_01.sql

En Oracle los usuarios necesitan permisos para poder acceder a la base de datos y a los objetos de la misma. Los privilegios pueden ser de dos tipos: a) del sistema y b) sobre objetos.

Para conceder un privilegio de sistema: çreate session", que es necesario para poder conectarse a la base de datos, es decir, para iniciar una sesión.

Pero teniendo únicamente este permiso, no podemos hacer mucho, solamente iniciar una sesión, pero no podemos crear tablas, ni ningún otro objeto; por ello son importantes los permisos de creación de objetos.

Los privilegios de sistema son permisos para realizar ciertas operaciones en la base de datos.

En Oracle existen dos tipos de privilegios de usuario:

* System: Que permite al usuario hacer ciertas tareas sobre la BD, como por ejemplo crear un Tablespace. Estos permisos son otorgados por el administrador o por alguien que haya recibido el permiso para administrar ese tipo de privilegio. Existen como 100 tipos distintos de privilegios de este tipo.
* Object: Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la BD, como una Tabla, Vista, un Procedure o Función, etc. Si a un usuario no se le dan estos permisos sólo puede acceder a sus propios objetos (véase USER_OBJECTS). Este tipo de permisos los da elowner o dueño del objeto, el administrador o alguien que haya recibido este permiso explícitamente (con Grant Option).

Los siguientes son algunos de los privilegios de sistema existentes:

* create session: para conectarse a la base de datos
* create table: crear tablas

* create sequence: crear secuencias;
* create view: crear vistas;
* create trigger: crear disparadores en su propio esquema;
* create procedure: crear procedimientos y funciones;
* execute any procedure: ejecutar cualquier procedimiento en cualquier esquema;
* create user: crear usuarios y especificar claves;
* create role: crear roles;
* drop user: eliminar usuarios.

Cada tipo de objeto tiene su propio conjunto de permisos:

* Tables: select, insert, update, delete, alter, debug, flashback, on commit refresh, query rewrite, references, all.
* Views: select, insert, update, delete, under, references, flashback, debug.
* Sequence: alter, select.
* Packeges, Procedures, Functions (Java classes, sources...): execute, debug.
* Materialized Views: delete, flashback, insert, select, update.
* Directories: read, write
* Libraries:execute
* User defined types: execute, debug, under
* Operators: execute
* Indextypes: execute

Concede permisos para objetos de sistema, como procedimientos almacenados del sistema, procedimientos almacenados extendidos, funciones y vistas.

```
GRANT { SELECT | EXECUTE } ON [ sys.]system_object TO principal
```

Argumentos

[sys.] .

Solo se requiere el calificador sys para hacer referencia a vistas de catálogo y vistas de administración dinámica.

system_object
Especifica el objeto en el que se va a conceder el permiso.
Especifica la entidad de seguridad para la que se concede el permiso.
Se asignan privilegios de sistema a un usuario mediante la instrucción "grant":

Sintaxis básica:

grant PERMISODESISTEMA
to USUARIO;

Oracle permite conceder múltiples privilegios a múltiples usuarios en una misma sentencia, debemos separarlos por comas.

En el siguiente ejemplo se concede el permiso para crear sesión a los usuarios "juanz .ªna":
grant create sesion to juan, ana;

En el siguiente ejemplo se conceden los permisos para crear tablas y vistas al usuario .ªna":
grant create table,
create view to ana;

En el siguiente ejemplo se conceden 2 permisos a 2 usuarios en una sola sentencia:
grant create trigger,
create procedure to juan, ana;

Consultando el diccionario "dba_sys_privs.ençontramos los privilegios concedidos a los distintos usuarios; y consultando üser_sys_privs.ºbtendremos la misma información pero únicamente del usuario actual.