Universidad Tecnológica de Panamá

Facultad de Ing. de Sistemas Computacionales

3er Año | Semestre II

Carrera: Ing. en Sistemas de información

Curso: Bases de Datos II

Profesor: Henry Lezcano

Investigación Final

Aseguramiento del Acceso a las Bases de Datos

Grupo: 1IF131

Fecha de Entrega: 10-11-2022

Índice

Cuentas de Usuario Bloqueadas y No Bloqueadas

Para efectos del Cursado de Sistemas de Bases de Datos II, en el Segundo Semestre Académico del Año 2022, dónde se ha impartido utilizando el lenguaje de Base de Datos PL/SQL, utilizaremos este como un elemento esencial de la investigación en curso, por lo que procederemos a describir ciertas tareas básicas de administración que se tienen que realizar para Gestionar los Usuarios de una Base de Datos PL/SQL:

- **Creación de Usuarios de Base de Datos**: A manera de que se vayan a crear usuarios en la base de datos, se debe conectar como usuario ADMIN, a través de cualquier herramienta de cliente SQL, sin embargo, una de las más utilizadas, ya sea en CLI (Command Line Interface) es SQLPLUS, mientras que a través del uso de una GUI (Graphical User Interface), Oracle recomienda el uso de SQL Developer, que en estos momentos se encuentra en su versión 16.
    - Al ejecutar la sentencia ***CREATE USER johel IDENTIFIED by contraseña;** así como GRANT CREATE SESSION TO johel; esto hace que se cree un nuevo usuario con privilegios de conexión a la Base de Datos, a lo que este puede ejecutar consultas, sin embargo, al no tener acceso de administrador total, se requieren temas como el otorgar privilegios adicionales al usuario en cuestión, lo cual es un tema que abordaremos posteriormente grosso modo.

Un tema de suma relevancia al momento de crear usuarios en una Base de Datos de tipo PL/SQL (Extrapolables a cualquier motor de Bases de Datos, es la creación de contraseñas seguras para sus usuarios, de manera que se han diseñado ciertas reglas de complejidad de contraseña por defecto:

- Todas las contraseñas deben poseer entre un mínimo de 12 y 30 caracteres de longitud, así como se debe incluir una letra en Mayúsculas, otra en Minúsculas y un Carácter Numérico.
- No se puede encontrar dentro de la contraseña, el nombre de usuario. Por ejemplo, si el nombre del usuario en cuestión es “johel”, la contraseña no podría ser “Johel273”, ya que esta a pesar del uso de las mayúsculas y minúsculas, incluye el nombre del usuario.
- Adicional a ello, es importante que, si se desea desbloquear la cuenta de un usuario específico en la Base de Datos, se debe conectar a ella como usuario ADMIN y ejecutar el siguiente comando: *ALTER USER username IDENTIFIED by contrasena ACCOUNT UNLOCK*

- **Eliminación de Usuarios en la Base de Datos**: Este es un tema especialmente prioritario al momento de asegurar los accesos, así como la autenticación de la Base de Datos, ya que se

espera que únicamente las personas autorizadas son las que puedan acceder a esta. Sin embargo, resulta importante reconocer que se vuelve una amenaza para la seguridad de la Empresa/Organización, al momento en el que por ejemplo se despide a un colaborador que tenía acceso a la Base de Datos, ya que, si sus accesos no han sido desactivados previamente a la notificación del despido, se pueden presentar situaciones complejas.

  - En PL/SQL, el proceso para eliminar un usuario de la Base de Datos requiere que nos conectemos como usuario ADMIN a través de cualquier herramienta de cliente SQL, se tiene que ejecutar la siguiente sentencia SQL:
    - *DROP USER nombre_usuario CASCADE;*
    - Esto hace que al nombre_usuario se elimine como usuario de la Base de Datos, así como se eliminan todos los objetos y datos que hayan sido creados o sean propiedad de él, por lo que debe manejarse con alto cuidado y verificación.

- **Gestión de Privilegios de Usuarios de Bases de Datos:** Existe un rol de Base de Datos predefinido en PL/SQL que se denomina DWROLE. El mismo se encarga de proporcionar los privilegios necesarios para la mayoría de los usuarios de la Base de datos, algunos de los privilegios que son otorgados a un usuario en cuestión, son la siguiente lista de sentencias SQL:
  - *CREATE ANALYTIC VIEW*
  - *CREATE ATTRIBUTE DIMENSION*
  - *ALTER SESSION*
  - *CREATE HIERARCHY*
  - *CREATE JOB*
  - *CREATE MINING MODEL*
  - *CREATE PROCEDURE*
  - *CREATE SEQUENCE*
  - *CREATE SESSION*
  - *CREATE SYNONYM*
  - *CREATE TABLE*
  - *CREATE TRIGGER*
  - *CREATE TYPE*
  - *CREATE VIEW*
  - *READ,WRITE ON directory DATA_PUMP_DIR*

Cuentas de Usuario y su Reestablecimiento

Los usuarios en general a nivel de PL/SQL se encuentran bloqueados al momento de fracasar sus diferentes intentos de inicio de sesión a través del subprograma conocido como “Identity Manager”, una de las causales que puede ser tomada en cuenta a razón de que un usuario quede bloqueado; es que este llegue a superar el número permitido de inicios de sesión fallidos, los cuales generan que las cuentas se bloqueen en cuestión, que manejan causales como las siguientes:

1. Los usuarios que superan el máximo de intentos fallidos de inicio de sesión con una contraseña quedarán bloqueados en todas las interfaces que existan de Identity Manager de Oracle, no excluyendo a la de recuperación de contraseña.
2. Los usuarios que superan el número máximo de intentos fallidos de inicio de sesión con una pregunta específica asignada por ellos mismos podrán autenticarse en todas las interfaces del subprograma de Identity Manager, con la debida excepción de las rutinas de recuperación de contraseña.

En estos casos, se conoce que el único capaz de hacerlo en una base de datos Oracle PL/SQL, vendría siendo el Administrador o aquel usuario que tenga todos los privilegios y permisos que hemos mencionado con anterioridad.

Por ejemplo, estas son las capacidades adecuadas que puede aplicar las operaciones siguientes al momento del bloqueo de una cuenta:

- **Actualizar**: Se pueden actualizar los datos generales de la cuenta, sin embargo, esto afectará directamente a los recursos y objetos que se encuentren en ella.
- **Cambiar o Reinicializar la Contraseña**: Este es el enfoque común, ya que en caso tal de que un usuario no recuerde su contraseña y la haya perdido por “N” motivo que pueda llegar a ser, se reconoce que la misma puede ser cambiada directamente por el Administrador o incluso, si la Base de Datos se encuentra conectada a internet en el servidor que está alojada, se le puede enviar un mal a este usuario con un Enlace Único, para el restablecimiento de su cuenta.
- **Inhabilitar o Habilitar**: De extrema importancia, ya que como fue mencionado en los comentarios iniciales de esta investigación por el autor de esta, se reconoce que muchas veces se presentarán casos de uso en los que se por un motivo específico, se deba inhabilitar automáticamente los accesos a un usuario X, pero en otro, habilitarlos.
- **Renombrar**

- **Desbloquear la Cuenta**

Usuarios Predeterminados de la Base de Datos

Existen algunos usuarios que al momento de la instalación del motor de Bases de Datos de Oracle PL/SQL, se proceden a crear de manera automática y a ellos se les otorga el rol de DBA (DataBase Administrator), ya que son usuarios administrados por el mismo sistema, como veremos a continuación; sin embargo, el acceso a cada uno de ellos, especialmente en el entorno gráfico, se convierte en uno de los principales problemas que se pueden presentar, a manera de asegurar la Base de Datos.

- **Usuario SYS**: Maneja una contraseña por defecto que es “CHANGE_ON_INSTALL”, es decir que se incita a que el usuario en cuestión, proceda a cambiarla automáticamente al momento de realizar la instalación, de forma que se puedan evitar brechas de seguridad.
    - Importante es reconocer que las tablas y vistas del Diccionario de Datos de la Base de Datos, se encuentran almacenadas en el Esquema (Schema en inglés) para el usuario SYS. Estas Tablas y Vistas son fundamentales para el funcionamiento de nuestra Base de Datos, ya que permiten mantener la Integridad del Diccionario de Datos, estas tablas son únicamente manipuladas por la base de datos.
        - Jamás se deben modificar o crear tablas en el Schema del usuario SYS.
- **Usuario SYSTEM**: Maneja una contraseña por defecto al momento de la instalación QUE ES “MANAGER”, por lo que también se recomienda cambiarlo de manera automática al momento de su instalación.
    - Dicho usuario, es utilizado principalmente para la creación de tablas y vistas adicionales que se encargan de mostrar información administrativa de la Base de Datos, especialmente tablas internas y vistas que se utilizan por varias opciones, así como herramientas de la misma Base de Datos Oracle.
        - Una buena práctica en general es el no uso del Schema SYSTEM para almacenar tablas o cualquier objeto general que sea de interés para usuarios no administrativos dentro de ella.

Es importante resaltar, que ninguno de los dos ejemplos de usuarios anteriormente mencionados, ni los que se encuentran en la Segunda Tabla de la siguiente imagen en cuestión (DBSNMP,

ORACLE_OCM, DIP, OUTLN, SYSTEM, SYS), pueden ser utilizados, ya que representan la integridad como tal de la instalación de PL/SQL, he ahí su buen uso e importancia.

Una buena práctica, resulta en no trabajar bajo ninguno de estos usuarios, sino como se muestra en la Primera Tabla, con usuarios creados, en muchos de los casos por el DBA (Database Administrator), como lo es en este caso el usuario '*johel*.

```
SQL> Select * from all_users;

USERNAME                       USER_ID CREATED
------------------------------ ---------- ---------
XS$NULL                      2147483638 29-MAY-14
johel                                49 02-NOV-22
APEX_040000                          47 29-MAY-14
APEX_PUBLIC_USER                     45 29-MAY-14
FLOWS_FILES                          44 29-MAY-14
HR                                   43 29-MAY-14
MDSYS                                42 29-MAY-14
ANONYMOUS                            35 29-MAY-14
XDB                                  34 29-MAY-14
CTXSYS                               32 29-MAY-14
APPQOSSYS                            30 29-MAY-14

USERNAME                       USER_ID CREATED
------------------------------ ---------- ---------
DBSNMP                               29 29-MAY-14
ORACLE_OCM                           21 29-MAY-14
DIP                                  14 29-MAY-14
OUTLN                                 9 29-MAY-14
SYSTEM                                5 29-MAY-14
SYS                                   0 29-MAY-14

17 rows selected.

SQL>
```

Figura N°2: En la segunda tabla se muestran todos los usuarios predeterminados que se encuentran cargados en cualquier tipo de Base de Datos PL/SQL

Administración de privilegios y funciones.

¿Qué es un privilegio?

Un privilegio es un derecho para gestionar un tipo particular de dictamen ó para acceder un objeto de otro usuario.

Un usuario puede aceptar los privilegios de dos maneras:

- Explícitamente
- Se asignan privilegios a un rol y posteriormente se asignan estos roles a uno o más usuarios.

El objetivo de los roles es otorgar una mejor administración de los privilegios, por lo general, se deberían garantizar privilegios a los roles y no a los usuarios individuales.

Tipos de Privilegios de Base de datos

Los privilegios de sistema más importantes:

Privilegio	Significado
CREATE SESSION	Permite al usuario conectar con la base de datos.
RESTRICTED SESSION	Permite al usuario establecer sesión con la base de datos en caso de que la base de datos esté en modo restringido mediante la instrucción: **ALTER SYSTEM ENABLE RESTRICTED SESSION** Sólo los usuarios con este privilegio pueden conectar con la base de datos si ésta se encuentra en este modo.
ALTER DATABASE	Permite modificar la estructura de la base de datos.
ALTER SYSTEM	Permite modificar los parámetros y variables del sistema.
CREATE TABLE	Permite crear tablas. Incluye la posibilidad de borrarlas.
GRANT ANY OBJECT PRIVILEGE	Permite conceder privilegios sobre objetos que no son del usuario (pertenecen a otros usuarios) a terceros usuarios.
CREATE ANY TABLE	Permite crear tablas en otros esquemas de usuario.
DROP ANY TABLE	Permite borrar tablas de otros usuarios.

SELECT ANY TABLE	Permite seleccionar datos en tablas de otros usuarios.
INSERT ANY TABLE	Permite añadir datos en tablas de otros usuarios.
UPDATE ANY TABLE	Permite eliminar datos en tablas de otros usuarios.
DELETE ANY TABLE	Permite eliminar datos en tablas de otros usuarios.

A continuación, una lista completa de privilegios:

Privilegio	Significado
Sesiones	
ALTER SESSION	Modificar el funcionamiento de la sesión
ALTER RESOURCE COST	Modifica los parámetros de cálculo de coste de la sesión
RESTRICTED SESSION	Conectar aunque la base de datos se haya iniciado en modo restringido
Base de datos y sistema	
ALTER DATABASE	Modificar la base de datos (privilegio de gran capacidad administrativa)
ALTER SYSTEM	Modificar los parámetros del sistema
AUDIT SYSTEM	Auditar la base de datos
Usuarios, roles, privilegios y perfiles	
CREATE USER	Crear usuarios pudiendo indicar tablespace por defecto, cuotas y perfiles
ALTER USER	Modificar al usuario. Permite cambiar la contraseña y modo de autentificación, tablespace por defecto, cuota de uso de disco, roles y el perfil del usuario
DROP USER	Borrar usuario
CREATE PROFILE	Crear perfiles
ALTER PROFILE	Modificar perfiles
DROP PROFILE	Borrar perfiles
CREATE ROLE	Crear roles
ALTER ANY ROLE	Modificar roles
GRANT ANY ROLE	Conceder roles
GRANT ANY PRIVILEGE	Conceder privilegios de sistema
Directorios	

CREATE ANY DIRECTORY	Crear directorios
DROP ANY DIRECTORY	Borrar directorios
Tablespaces (espacios de tabla)	
CREATE TABLESPACES	Crear tablespaces
ALTER TABLESPACE	Modificar tablespaces
DROP TABLESPACE	Borrar tablespaces
MANAGE TABLESPACE	Administrar el espacio de tablas para poder hacer copia de seguridad o simplemente quedar online u offline el tablespace
UNLIMITED TABLESPACE	Usa cuota ilimitada al escribir en cualquier tablespace. Este privilegio elimina las cuotas establecidas sobre el usuario, si las hubiera.
Tablas	
CREATE TABLE	Crear tablas en el esquema del usuario, incluye insertar, modificar y eliminar datos de la misma; así como eliminar la propia tabla
ALTER ANY TABLE	Modificar tablas de cualquier usuario
BACKUP ANY TABLE	Utilizar la utilidad **Export** para copiar datos de otros esquemas.
CREATE ANY TABLE	Crear tablas en cualquier esquema
DELETE ANY TABLE	Borrar filas de tablas en cualquier esquema
DROP ANY TABLE	Borrar tablas en cualquier esquema
INSERT ANY TABLE	Añadir datos a cualquier tabla
SELECT ANY TABLE	Seleccionar datos de tablas en cualquier esquema
UPDATE ANY TABLE	Modificar datos de tablas de cualquier esquema
LOCK ANY TABLE	Bloquear tablas, vistas e instantáneas en cualquier esquema

FLASHBACK ANY TABLE	Realizar acción de flashback en tablas, vistas e instantáneas en cualquier esquema
Vistas	
CREATE VIEW	Crear vistas en el esquema del usuario
CREATE ANY VIEW	Crear vistas en cualquier esquema
DROP ANY VIEW	Borrar cualquier vista en cualquier esquema
UNDER ANY VIEW	Crear subvistas
Instantáneas (Snapshots o vistas materializadas)	
CREATE MATERIALIZED VIEW	Crear vistas materializadas (instantáneas)
CREATE ANY MATERIALIZED VIEW	Crear vistas materializadas (instantáneas) en cualquier esquema
ALTER ANY MATERIALIZED VIEW	Modificar vistas materializadas (instantáneas) en cualquier esquema
DROP ANY MATERIALIZED VIEW	Borrar vistas materializadas (instantáneas) en cualquier esquema
GLOBAL QUERY REWRITE	Permite realizar operaciones de lectura escritura en instantáneas que usan tablas de otros esquemas
CREATE SNAPSHOT	Crear instantáneas (obsoleto)
ALTER ANY SNAPSHOT	Modificar instantáneas de cualquier usuario (obsoleto)
CREATE ANY SNAPSHOT	Crear instantáneas a cualquier usuario (obsoleto)
DROP ANY SNAPSHOT	Borrar instantáneas (obsoleto)
PL/SQL	
CREATE PROCEDURE	Crear procedimientos y funciones PL/SQL

ALTER ANY PROCEDURE	Modificar procedimientos y funciones de cualquier usuario
CREATE ANY PROCEDURE	Crear funciones y procedimientos en cualquier esquema
DROP ANY PROCEDURE	Borrar cualquier procedimiento en cualquier esquema
EXECUTE ANY PROCEDURE	Ejecutar cualquier procedimiento en cualquier esquema
CREATE TRIGGER	Crear triggers
ALTER ANY TRIGGER	Modificar triggers de cualquier usuario
CREATE ANY TRIGGER	Crear triggers en cualquier esquema
DROP ANY TRIGGER	Borrar triggers de cualquier esquema
ADMINISTER DATABASE TRIGGER	Crear triggers de sistema (requiere además el privilegio **CREATE TRIGGER**)
CREATE LIBRARY	Crear librerías de procedimientos y funciones en el esquema de usuario
CREATE ANY LIBRARY	Crear librerías de procedimientos y funciones en cualquier esquema
DROP ANY TRIGGER	Borrar cualquier trigger
DROP LIBRARY	Borrar librería de procedimientos y funciones en el esquema de usuario
DROP ANY LIBRARY	Borrar librerías de procedimientos y funciones en cualquier esquema
EXECUTE ANY LIBRARY	Ejecutar cualquier librería
Tipos de datos	
CREATE TYPE	Crear tipos de datos personales
ALTER ANY TYPE	Modificar tipos de datos personales en cualquier usuario
CREATE ANY TYPE	Crear tipos de datos en cualquier esquema
DROP ANY TYPE	Borrar tipos de datos de cualquier esquema

EXECUTE ANY TYPE	Permite invocar a tipos de datos personales presentes en cualquier esquema
Índices	
ALTER ANY INDEX	Modificar índices de la base de datos (incluye modificar claves primarias, secundarias,…)
CREATE ANY INDEX	Crear índices en cualquier esquema
DROP ANY INDEX	Borrar índices en cualquier esquema
Secuencias y sinónimos	
ALTER ANY SEQUENCE	Modificar secuencias de cualquier usuario
CREATE ANY SEQUENCE	Crear secuencias en cualquier esquema
CREATE ANY SYNONYM	Crear sinónimos en cualquier esquema
CREATE SEQUENCE	Crear secuencias
CREATE SYNONYM	Crear sinónimos
CREATE PUBLIC SYNONYM	Crear sinónimos públicos
DROP PUBLIC SYNONYM	Borrar sinónimos públicos
CREATE ANY SEQUENCE	Crear secuencias en cualquier esquema
DROP ANY SEQUENCE	Borrar secuencias en cualquier esquema
DROP ANY SYNONYM	Borrar sinónimos en cualquier esquema
SELECT ANY SEQUENCE	Seleccionar cualquier secuencia de cualquier esquema
Clusters	
CREATE CLUSTER	Crea y modifica clusters en el esquema actual

ALTER ANY CLUSTER	Modificar clusters
CREATE ANY CLUSTER	Crear clusters en cualquier esquema
DROP ANY CLUSTER	Borrar cualquier cluster
Segmentos de rollback	
CREATE ROLLBACK SEGMENT	Crear segmentos de rollback
ALTER ROLLBACK SEGMENT	Modificar segmentos de rollback
DROP ROLLBACK SEGMENT	Borrar segmento de rollback
Enlaces a base de datos	
CREATE DATABASE LINK	Crear enlaces privados a bases de datos en el esquema del usuario
CREATE PUBLIC DATABASE LINK	Crear enlaces públicos a bases de datos
CREATE DATABASE LINK	Modificar enlaces privados a bases de datos
CREATE PUBLIC DATABASE LINK	Modificar enlaces públicos a bases de datos
DROP PUBLIC DATABASE LINK	Borrar enlaces públicos a bases de datos
Programación de tareas	
CREATE JOB	Crear trabajo planificado en el esquema actual
CREATE ANY JOB	Crea, modifica y elimina tareas, programas y credenciales de cualquier esquema (excepto SYS). Esto permite ejecutar código en cualquier esquema de cualquier usuario.
CREATE EXTERNAL JOB	Crear un trabajo en el esquema de usuario procedente del planificador de tareas del sistema operativo

EXECUTE ANY PROGRAM	Ejecutar cualquier programa presente en un trabajo planificado del esquema de usuario.
EXECUTE ANY CLASS	Asignar cualquier clase a un trabajo en el esquema de usuario.
MANAGE SCHEDULER	Administrar el planificador de tareas,
Varios	
ANALYZE ANY	Analizar cualquier tabla, clúster o índice en cualquier esquema.
ANALYZE ANY DICTIONARY	Analizar cualquier elemento del diccionario de datos
SELECT ANY DICTIONARY	Realizar SELECT sobre las vistas del diccionario de datos
AUDIT ANY	Auditar a cualquier objeto de la base de datos
BECOME USER	Convertirse en otro usuario al utilizar algunas de las utilidades de Oracle
COMMENT ANY TABLE	Realizar comentarios sobre tablas, columnas y vistas en cualquier esquema de la base de datos
SELECT ANY TRANSACTION	Seleccionar los datos de la vista **FLASHBACK_TRANSACTION_QUERY** que controla el proceso de la actual operación flashback.
FORCE ANY TRANSACTION	Forzar aceptar (**COMMIT**) las transacciones en duda en un sistema distribuido de bases de datos en cualquier conexión
FORCE TRANSACTION	Forzar aceptar (**COMMIT**) la transacción actual en caso de duda.
SYSDBA	Privilegio general de administrador
Varios	
SYSOPER	Privilegio general de administrador (más bajo que el anterior)
FLASHBACK ARCHIVE ADMINISTER	Crea, elimina o modifica cualquier archivo de flashback
DEBUG CONNECT SESSION	Conectar la sesión a un depurador
DEBUG ANY PROCEDURE	Conectar procedimientos, funciones y/o código Java a un depurador

Conceder y restaurar privilegios de usuario

Para conceder privilegios se usa la instrucción **GRANT** que se verá a continuación en el siguiente formato.

```
GRANT privilegio1 [,privilegio2[,…]] TO usuario
[WITH ADMIN OPTION];
```

Adicional se usó el **WITH ADMIN OPTION** que permite al usuario que se le dio el privilegios de poder dar esos privilegios a otros usuarios.

A continuación, un ejemplo de uso.

```
GRANT   CREATE SESSION, ALTER SESSION, CREATE TABLE,
CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE,
CREATE TRIGGER, CREATE PROCEDURE, CREATE TYPE
TO emarchena;
```

Administración de privilegios con tareas

Los privilegios permiten a los usuarios realizar tareas con derechos administrativos y también sirven para crear límites para que el usuario solo realice las tareas permitidas.

Para realizar la tarea de **visualizar los nombres y las definiciones de privilegios** se podría usar el siguiente formato que es utilizado por desarrolladores:

% **man privileges**

Para **determinar los privilegios que se le asignaron directamente** se realiza el siguiente procedimiento:

1. Enumerar los privilegios que los procesos pueden utilizar.

Consulte Cómo determinar los privilegios de un proceso para conocer el procedimiento.

2. Invocar acciones y ejecutar comandos en cualquier shell.

Los privilegios que se muestran en el conjunto vigente están en vigor a lo largo de la sesión. Si se le asignaron privilegios directamente, además del conjunto básico, los privilegios se muestran en el conjunto vigente.

A continuación, un ejemplo de uso en el cual se asignó el privilegio proc_clock_highres directamente al usuario por lo que este está disponible en todos los procesos que son propiedad del usuario:

% **ppriv -v $$**

1800: pfksh

flags = <none>

E: file_link_any,…,**proc_clock_highres**,proc_session

I: file_link_any,…,**proc_clock_highres**,proc_session

P: file_link_any,…,**proc_clock_highres**,proc_session

L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,…,sys_time

% **ppriv -vl proc_clock_highres**

Allows a process to use high resolution timers.

Para **determinar los comandos con privilegios que puede ejecutar,** por lo general se tiene acceso a comandos con privilegios mediante un perfil de derechos. Los comandos de un perfil de derechos se deben ejecutar en un shell de perfil. Para esto se realiza el siguiente procedimiento:

1. **Determinar los perfiles de derechos que se le asignaron:**

En el siguiente ejemplo, se asigna al usuario varios perfiles de derechos. El sistema lee los perfiles de derechos y su contenido en orden. Para todos los atributos excepto las autorizaciones, el primer valor de atributo definido explícitamente es el que se utiliza. Para obtener más información, consulte Orden de búsqueda para atributos de seguridad asignados.

% **profiles**

- Audit Review
- Console User
- Suspend To RAM
- Suspend To Disk
- Brightness
- CPU Power Management
- Network Autoconf
- Desktop Print Management
- Network Wifi Info

- Desktop Removable Media User
- Basic Solaris User
- All

2. **Determinar sus derechos del perfil de revisión de auditoría,** como se ve en el siguiente ejemplo:

profiles -l

Audit Review

solaris.audit.read

/usr/sbin/auditreduce euid=0

/usr/sbin/auditstat euid=0

/usr/sbin/praudit euid=0

En el siguiente ejemplo de la determinación de comandos con privilegios de un rol, un usuario asume un rol asignado y enumera los comandos que se incluyen en uno de los perfiles de derechos:

% **roles**

devadmin

% **su - devadmin**

Password: Type devadmin password

$ **profiles -l**

Device Security

```
        /usr/bin/kbd        uid=0;gid=sys
        /usr/sbin/add_allocatable    euid=0
        /usr/sbin/add_drv        uid=0
        /usr/sbin/devfsadm        uid=0
        /usr/sbin/eeprom        uid=0
        /usr/sbin/list_devices        euid=0
        /usr/sbin/rem_drv        uid=0
        /usr/sbin/remove_allocatable    euid=0
```

```
/usr/sbin/strace        euid=0
/usr/sbin/update_drv        uid=0
```

Para **determinar los privilegios de un proceso,** se enumeran los privilegios que están disponibles para el proceso del shell:

En el siguiente ejemplo se enumeran los privilegios del proceso principal del shell del usuario:

% **ppriv $$**

1200: -csh

flags = <none>

E: basic

I: basic

P: basic

L: all

% **ppriv -v $$**

1200: -csh

flags = <none>

E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session

I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session

P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session

L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,…,sys_time

Para determinar los privilegios que necesita un programa, se realiza el siguiente procedimiento:

1. **Escribir el comando con errores como un argumento del comando de depuración ppriv.**

   % **ppriv -eD touch /etc/acct/yearly**

   touch[5245]: missing privilege "file_dac_write"

   (euid = 130, syscall = 224) needed at zfs_zaccess+0x258

   touch: cannot create /etc/acct/yearly: Permission denied

2. **Determinar qué llamada del sistema falla, busque el número syscall en el archivo /etc/name_to_sysnum.**

% **grep 224 /etc/name_to_sysnum**

creat64 224

En el siguiente ejemplo se utiliza el comando truss para examinar el uso de privilegios:

% **truss -t creat touch /etc/acct/yearly**

creat64("/etc/acct/yearly", 0666)

Err#13 EACCES [**file_dac_write**]

touch: /etc/acct/yearly cannot create

Para **aplicar una política de privilegio extendida a un puerto**, se realiza el siguiente procedimiento:

1. **Leer la entrada de manifiesto de servicio predeterminada para el puerto.**

Desde la siguiente entrada /lib/svc/manifest/network/ntp.xml, los privilegios net_privaddr, proc_lock_memory y sys_time pueden utilizarse en otros procesos.

privileges='basic,!file_link_any,!proc_info,!proc_session,

net_privaddr,proc_lock_memory,sys_time'

Los privilegios eliminados evitan que el servicio indique u observe cualquier otro proceso, y evitan la creación de enlaces físicos como una manera de renombrar archivos.

Es decir, el proceso que inicia el servicio solamente se puede enlazar con el puerto específico 123, y no se puede enlazar con ningún otro puerto con privilegios. Si un pirata informático quisiera aprovechar el servicio para iniciar otro proceso, el proceso secundario no podría establecer un enlace a ningún otro puerto con privilegios.

2. **Limitar el privilegio net_privaddr a este puerto solamente.**

La política de privilegio extendida, que aparece resaltada en el siguiente fragmento, impide el acceso de este servicio a otros puertos con privilegios:

privileges='basic,!file_link_any,!proc_info,!proc_session,

{net_privaddr}:123/udp,proc_lock_memory,sys_time'

Para **ejecutar una secuencia de comandos de Shell con comandos con privilegios**, se realiza el siguiente procedimiento:

1. **Iniciar la secuencia de comandos con /bin/pfsh, o cualquier otro shell de perfil, en la primera línea.**

   #!/bin/pfsh

   # Copyright (c) 2022 by UTP

2. **Determinar los privilegios que necesitan los comandos de la secuencia de comandos.**

   % ppriv -eD *script-full-path*

3. **Convertirse en administrador con los atributos de seguridad necesarios.**

4. **Crear o modificar un perfil de derechos para la secuencia de comandos.**

   Hay que Agregar la secuencia de comandos de shell y los comandos en la secuencia de comandos de shell con sus atributos de seguridad necesarios al perfil de derechos.

5. **Agregar el perfil de derechos a un rol y asignar el rol a un usuario.**

Para ejecutar la secuencia de comandos, el usuario asume el rol y ejecuta la secuencia de comandos en el shell de perfil del rol.

Límites de recurso de base de datos

Cuotas de espacio de tablas

Para establecer límites en la cantidad de almacenamiento que puede usar un usuario o grupo de usuarios se utilizan las cuotas. Se pueden establecer cuotas en los niveles de sistema de archivos, sistema, red, base de datos, tablespace e instancia.

Los siguientes pasos describen cómo funcionan las cuotas.

1. El escaneo recopila mucha información sobre los recursos de almacenamiento de la empresa. Dicha información se almacena en bases de datos.
2. Cuando se ejecuta un trabajo de cuota, verifica la información de inventario para determinar si hay alguna infracción de cuota. Si hay una infracción, se activa una alarma y se toman las medidas adecuadas.

Se pueden definir dos tipos diferentes de cuotas: usuarios y grupos de usuarios del sistema operativo.

Cuota de uso: seleccionar usuarios y grupos de usuarios para cuotas definidas.

Cuota del grupo de usuarios del sistema operativo: Se debe seleccionar el grupo de usuarios del sistema operativo de cuota. Los grupos de usuarios del sistema operativo son grupos de usuarios definidos en el

sistema operativo. Se pueden crear grupos que contengan muchos grupos de usuarios del sistema operativo. Al crear dichas cuotas, puede seleccionar un solo grupo de usuarios de SO y un grupo de varios grupos de usuarios de SO.

La capacidad de definir cuotas en diferentes niveles le permite controlar con precisión el almacenamiento disponible para un usuario o grupo de usuarios en un sistema de archivos, sistema, red, base de datos, espacio de tabla e instancia determinados:

Sistema de archivos: Se deben establecer límites de uso de almacenamiento para sistemas de archivos específicos y grupos de sistemas de archivos. Se recibirá una alerta si un usuario o grupo de usuarios supera el límite de uso de almacenamiento que ha definido para un sistema de archivos específico o un grupo de sistemas de archivos en la cuota.

Sistema: Se deben establecer límites de uso de almacenamiento para sistemas específicos y grupos de sistemas de archivos. Se recibirá una alerta si un usuario o grupo de usuarios excede el límite de uso de almacenamiento que ha definido para un sistema específico o grupo de sistemas en una cuota.

Espacio de tabla de la base de datos: Es necesario el establecimiento de límites de uso de almacenamiento para bases de datos, espacios de tablas, grupos de bases de datos y grupos de espacios de tablas específicos. Recibirá una alerta si un usuario o grupo de usuarios supera los límites de uso de almacenamiento establecidos para estos recursos de almacenamiento de cuota.

Instancia: Se establecen límites de uso de almacenamiento para instancias, sistemas y grupos de sistemas de archivos específicos. Recibirá una alerta si un usuario o grupo de usuarios supera los límites de uso de almacenamiento que defina para instancias, sistemas y grupos de sistemas específicos en su cuota.

La red: Establecimiento de límites de uso de almacenamiento a nivel de red para múltiples sistemas, grupos de sistemas, sistemas de archivos, bases de datos y tablespaces de red.

Por default ningun usuario tiene una cuota en los tablespaces y se tienen tres opciones para poder proveer a un usuario de una cuota:

- Sin límite, que permite al usuario usar todo el espacio disponible de un tablespace.
- Por medio de un valor, que puede ser en kilobytes o megabytes que el usuario puede usar. Este valor puede ser más grande que el table space o más chico
- Por medio del privilegio UNLIMITED TABLESPACE, el cuál va a pesar más que cualquier cuota dada en un tablespace por lo que tienen disponibilidad de todo el espacio incluyendo en SYSTEM y SYSAUX.

Como recomendación, no se deben de dar cuotas a los usuarios en los tablespaces de SYSTEM y SYSAUX, pues tipicamente solo los usuarios de SYS y SYSTEM pueden crear objetos en estos. También no dar cuotas en su tablespace temporal o del tipo undo.

Perfiles de límite de recursos

Los perfiles de usuario son utilizados para restringir la cantidad de recursos del sistema y de la base de datos que puede emplear un usuario. Si el administrador de la base de datos no crea los perfiles para un usuario, estos usarán el perfil por defecto en donde los recursos para este serán infinitos. Los límites que se les pueden establecer van desde indicar la cantidad de segundos que los usuarios estarán inactivos en la base de datos antes de desconectarse hasta cantidad de intentos fallidos por ingresar una contraseña incorrecta.

Entre los recursos más relevantes que se le puede limitar a un usuario por un perfil están los siguientes:

Recursos	Descripción
SESSIONES_PER_USER	El número de sesiones concurrentes que un usuario puede tener en una instancia.
CPU_PER_SESSION	El tiempo de CPU, en centenas de segundos, que una sesión puede utilizar.
CONNECT_TIME	El número de minutos que una sesión puede permanecer activa.
IDLE_TIME	El número de minutos que una sesión puede permanecer sin que sea utilizada de manera activa.
LOGICAL_READS_PER_SESSION	El número de bloques de datos que se pueden leer en una sesión.
LOGICAL_READS_PER_CALL	El número de bloques de datos que se pueden leer en una operación.
PRIVATE_SGA	La cantidad de espacio privado que una sesión puede reservar en la zona de SQL compartido de la SGA.
COMPOSITE_LIMIT	El número de total de recursos por sesión, en unidades de servicio. Esto resulta de un cálculo ponderado de CPU_PER_SESSION, CONNECT_TIME, LOGICAL_READS_PER_SESSION y PRIVATE_SGA, cuyos pesos se pueden variar con el comando ALTER RESOURCE COST.

Creación de un perfil

Para crear un perfil es necesario que el usuario que lo va a crear posea el privilegio CREATE PROFILE, y se empleara siguiente comando mostrado:

create profile nombre_perfil limit
nombre_limite_1 [valor entero | unlimited | default]
nombre_limite_2 [valor entero | unlimited | default]
...
nombre_limite_n [valor entero | unlimited | default];

La palabra ‘unlimited’ indica que todos los perfiles creados tienen recursos sin límites. Como se menciono anteriormente si no se crean los perfiles, todos los usuarios de la base de datos tomaran el perfil por ‘default’, el cual cuenta con todos los recursos. Además, si a los limites no se les asigna un valor predefinido tomaran el valor del perfil por defecto, como se aprecia en este ejemplo:

```
SQL> create profile lim_prueba limit connect_time 45;

Profile created.

SQL> select *
  2  from   dba_profiles
  3  where  profile = 'LIM_PRUEBA'
  4  order by resource_name;

PROFILE              RESOURCE_NAME              RESOURCE LIMIT
-------------------- -------------------------- -------- ----------------
LIM_PRUEBA           COMPOSITE_LIMIT            KERNEL   DEFAULT
LIM_PRUEBA           CONNECT_TIME               KERNEL   45
LIM_PRUEBA           CPU_PER_CALL               KERNEL   DEFAULT
LIM_PRUEBA           CPU_PER_SESSION            KERNEL   DEFAULT
LIM_PRUEBA           FAILED_LOGIN_ATTEMPTS      PASSWORD DEFAULT
LIM_PRUEBA           IDLE_TIME                  KERNEL   DEFAULT
LIM_PRUEBA           LOGICAL_READS_PER_CALL     KERNEL   DEFAULT
LIM_PRUEBA           LOGICAL_READS_PER_SESSION  KERNEL   DEFAULT
LIM_PRUEBA           PASSWORD_GRACE_TIME        PASSWORD DEFAULT
```

Modificar un perfil

Para modificar un perfil se necesita el privilegio ALTER PROFILE, con el cual se podrá modificar o asignar valores a los límites de los perfiles creados.

```
SQL> alter profile lim_prueba limit password_life_time 30;
Profile altered.

SQL> select *
  2  from   dba_profiles
  3  where  profile = 'LIM_PRUEBA'
  4  order by resource_name;

PROFILE              RESOURCE_NAME             RESOURCE LIMIT
-------------------- ------------------------- -------- ---------------
LIM_PRUEBA           COMPOSITE_LIMIT           KERNEL   DEFAULT
LIM_PRUEBA           CONNECT_TIME              KERNEL   45
LIM_PRUEBA           CPU_PER_CALL              KERNEL   DEFAULT
LIM_PRUEBA           CPU_PER_SESSION           KERNEL   DEFAULT
LIM_PRUEBA           FAILED_LOGIN_ATTEMPTS     PASSWORD DEFAULT
LIM_PRUEBA           IDLE_TIME                 KERNEL   DEFAULT
LIM_PRUEBA           LOGICAL_READS_PER_CALL    KERNEL   DEFAULT
LIM_PRUEBA           LOGICAL_READS_PER_SESSION KERNEL   DEFAULT
LIM_PRUEBA           PASSWORD_GRACE_TIME       PASSWORD DEFAULT
LIM_PRUEBA           PASSWORD_LIFE_TIME        PASSWORD 30
LIM_PRUEBA           PASSWORD_LOCK_TIME        PASSWORD DEFAULT
LIM_PRUEBA           PASSWORD_REUSE_MAX        PASSWORD DEFAULT
LIM_PRUEBA           PASSWORD_REUSE_TIME       PASSWORD DEFAULT
```

Borrar un perfil

Para borrar un perfil se utilizará el comando DROP como con otros objetos en Oracle. Es fundamental recordar que si este perfil esta asignado a otros usuarios debemos colocar ‘cascade’ para que sea eliminado de ellos también.

drop profile nombre_perfil

```
SQL> drop profile lim_prueba;
Profile dropped.
SQL> select *
  2  from   dba_profiles
  3  where  profile = 'LIM_PRUEBA'
  4  order by resource_name;
no rows selected
```

Asignar un perfil a un usuario

Una vez creado el perfil, estos pueden ser asignados con el comando ALTER USER o en el instante que son creados con CREATE USER.

```
alter user nombre_usuario profile nombre_perfil;

create user nombre_usuario
identified by        password_usuario
default tablespace   nombre_tbs
temporary tablespace nombre_tbs
profile              nombre_perfil;
```

Y si se desea designar el perfil a un usuario, solo se debe asignar el perfil por defecto a este:

```
SQL> alter user curso profile default;
User altered.
SQL> select username, default_tablespace, temporary_tablespace, profile
  2  from   dba_users
  3  where  username = 'CURSO';
USERNAME             DEFAULT_TABLESPACE        TEMPORARY_TABLESPACE
-------------------- ------------------------- -------------------------
CURSO                DATOS                     TEMP
```

ADMINISTRACIÓN DE CUENTAS DE USUARIOS

Todo acceso a la base de datos requiere un inicio de sesión con un nombre de usuario y una contraseña. A este usuario se les otorgará acceso a ciertos objetos de la base de datos, pero se le restringirá (a menos que sea un superadministrador) el uso de otros. A un usuario se le asigna un conjunto de permisos que otorga permiso para usar ciertos objetos. Estos permisos a menudo se agrupan en los llamados roles, que le permiten estructurar mejor los permisos otorgados a los usuarios. Un perfil de usuario será un conjunto de permisos y restricciones que se aplican a ese usuario.

Por ello, cuando un usuario se conecta, debe acreditar que es quien dice ser (normalmente a través de una contraseña), es decir, que está autenticado. Por otro lado, dicha aprobación crea privilegios (derechos) y restricciones.

En el caso de la base de datos de Oracle posee dos privilegios de sistema asociados a tareas administrativas cuales son:

- SYSDBA: que posee la capacidad de parar e iniciar la instancia de base de datos; modificar la base de datos, crear y borrar bases de datos, Crear el archivo de parámetros, cambiar el

modo de archivado de la base de datos, recuperar la base de datos y además incluye el privilegio de sistema RESTRICTED SESSION.

- SYSOPER: que posee la mismas capacidades y permisos que el SYSDBA, solo con la diferencia que puede: crear y borrar la base de datos y recuperar en todas las formas la base de datos.

A los usuarios de la base de datos de Oracle se les puede asignar la configuración referida a:

- Nombre de usuario, que este no puede repetirse y como máximo debe tener 30 caracteres que sólo podrán contener letras del alfabeto inglés, números, el signo dólar y el signo de guión bajo.
- Configuración física, la cual es el espacio asociado al usuario para almacenar sus datos y la cuota que se le asigna a dicho usuario y mediante la que se establece el espacio máximo que el usuario puede gastar para almacenar los datos.
- Perfil asociado, el usuario indica los recursos y configuración que tomará el usuario al sistema.
- Privilegios y roles, permiten especificar los permisos que posee el usuario.
- Estado de la cuenta de usuario:
    - Abierta: el usuario puede conectar y realizar sus acciones habituales
    - Bloqueada. el usuario no podrá conectar mientras siga en estado bloqueado.
    - Expirada. La cuenta agotó el tiempo máximo asignado a ella. Para salir de este estado, el usuario/a debe resetear su contraseña de usuario.

PERFIL PREDETERMINADO

El software de base de datos Oracle incluye funciones para proporcionar a los usuarios un acceso de base de datos segura. El servidor de Oracle genera automáticamente un perfil por defecto cuando se crea la base de datos. Un perfil es un conjunto con nombre de los parámetros de las contraseñas y los límites de recursos de base de datos, como la caducidad de la contraseña, reglas de verificación de complejidad de contraseña, y conectar las cuotas de tiempo.

El perfil predeterminado tiene dos funciones:

- Para actuar como el perfil predeterminado para un usuario donde no se especifica ningún perfil
- Para actuar como una definición de valores predeterminados para otros perfiles

Cualquiera de los parámetros documentados anteriormente puede tener un valor predeterminado DEFAULT. Oracle utiliza el valor especificado en el perfil DEFAULT para ese parámetro. Este proceso

se repite cada vez que un usuario se conecta, por lo que un cambio en el perfil DEFAULT automáticamente tendrá efecto con la próxima conexión.

Al cambiar la configuración de contraseña y limitar en el perfil predeterminado con el ALTER COMANDO y VERIFY_FUNCTION PL / SQL puede asignar los límites de validación y de recursos de base de datos de contraseñas a usuarios particulares.

El perfil llamado DEFAULT se aplica automáticamente a todos los usuarios y les da recursos ilimitados sobre la base de datos.

ADMINISTRAR PERFILES DE LÍMITE RECURSOS

Para limitar el número de recursos se debe de activar (poniéndola el valor TRUE) la variable de sistema RESOURCE_LIMIT (que por defecto está a FALSE).

Perfiles relacionados con el uso de recursos. Establecen el máximo o mínimo uso de recursos de la base de datos por parte del usuario.

Variable de perfil	Significado
SESSIONS_PER_USER	Número de conexiones de usuario concurrentes que se permiten.
CPU_PER_SESSION	Límite de tiempo (en centésimas de segundo) que se permite a un usuario utilizar la CPU antes de ser echado del sistema. De esa forma se evitan peligros de rendimiento
CPU_PER_CALL	Como la anterior pero referida a cada proceso
PRIVATE_SGA	Para conexiones en instalaciones de servidor compartido, número de KB que puede consumir cada sesión en la zona de memoria compartida (**SGA**)
CONNECT_TIME	Minutos como máximo que se permite a una sesión
IDLE_TIME	Minutos máximos de inactividad de una sesión
LOGICAL_READS_PER_SESSION	Máximo número de bloques leídos en una sesión

LOGICAL_READS_PER_CALL	Máximo número de bloques leídos por un proceso
COMPOSITE_LIMIT	Máximo número de recursos consumidos por una sesión. Es la media ponderada de varios parámetros anteriores

CREAR PERFILES

Sintaxis:

```
CREATE PROFILE perfil LIMIT parámetro1 valor1
[parametro2 valor [...]]
```

Los parámetros por especificar son los que aparecen en la tabla anterior. A cada parámetro se le indica un valor, o bien la palabra **DEFAULT** si deseamos que tome su valor por defecto, o bien **UNLIMITED** para indicar que el parámetro tomará un valor de infinito.

Ejemplo:

```
CREATE PROFILE programador LIMIT
    SESSIONS_PER_USER UNLIMITED
    CPU_PER_SESSION UNLIMITED                IDLE_TIME
15       CONNECT_TIME 150      FAILED_LOGIN_ATTEMPTS
5        PASSWORD_LOCK_TIME 2;
```

Respaldo y Recuperación de una base de datos.

Tener un respaldo garantiza que los datos estén seguros y que la información crítica no se pierda. Esto aplica para desastres naturales, robo de datos o cualquier otro tipo de emergencia. De esta manera entender que las copias de seguridad o **respaldos** se consideran como el proceso mediante el que se duplican datos importantes. Permitiendo la recuperación de este conjunto en un momento determinado. (Montenegro, 2021).

Debemos entender que una correcta **recuperación** de los datos a tiempo, como menciona (Toledo, 2022) en la web de CIBERNOS GRUPO, permitirá: Reanudar las operaciones de la empresa lo antes posible. Mantener las conexiones con los principales clientes o proveedores de la organización. Evitar pérdidas económicas y de reputación.

Cómo hacer una copia de seguridad de la base de datos de Oracle con PL / SQL

PL/SQL Developer Base de datos Oracle. Las principales herramientas utilizadas para importar o exportar bases de datos que se han de presentar a continuación, detallan principalmente el proceso de importación y exportación de bases de datos usando PL / SQL Developer,

Pasos de exportación:

1 herramientas -> exportar objeto de usuario Seleccione la opción para exportar el archivo .sql.

2 herramientas -> exportar tablas-> Oracle Export Seleccione la opción para exportar archivos .dmp.

Importar pasos:

Nota: Es mejor eliminar la tabla anterior antes de importar, excepto, por supuesto, importar otra base de datos.

1 herramientas-> importar tablas-> SQL Inserts importar archivos .sql.

2 herramientas-> importar talbes-> Importar Oracle y luego importar el archivo dmp.

Algunas notas:

Lo que Herramientas-> Exportar objetos de usuario exportar es crear una declaración de tabla (incluida la estructura de almacenamiento). Este método solo puede exportar tablas que pertenecen a este usuario, y las tablas de otros usuarios no se pueden exportar, se recomienda exportar usando la línea de comando (exp, imp).

Herramientas-> Exportar tablas contiene tres métodos de exportación, los tres métodos pueden exportar la estructura y los datos de la tabla, de la siguiente manera:

- Oracle Export
- Sql Insert
- pl/sql developer

El primero es el formato de archivo exportado como .dmp. El archivo .dmp es binario, puede ser multiplataforma, también puede contener permisos, es muy eficiente y es el más utilizado.

El segundo tipo se exporta como un archivo .sql, que se puede ver con un editor de texto. Tiene mayor versatilidad, pero la eficiencia no es tan buena como el primer tipo. Es adecuado para la importación y exportación de datos pequeños. Especialmente tenga en cuenta que no puede haber campos grandes (blob,

clob, long) en la tabla. Si los hay, le indicará que no se puede exportar (el mensaje es el siguiente: la tabla contiene una o más columnas LONG que no se pueden exportar en formato sql, en su lugar, el formato de desarrollador Pl / sql del usuario) .

El tercero es exportar a formato .pde. .Pde es el formato de archivo propio del desarrollador Pl / sql, que solo puede ser importado y exportado por el desarrollador Pl / sql y no puede verse con un editor.

Solo después de exportar y luego importar el método "Oracle Export", la estructura de la tabla y la estructura del índice no han cambiado, y los otros dos métodos han cambiado el tipo de índice.

Exportar objetos y datos.

a) Exportación de datos

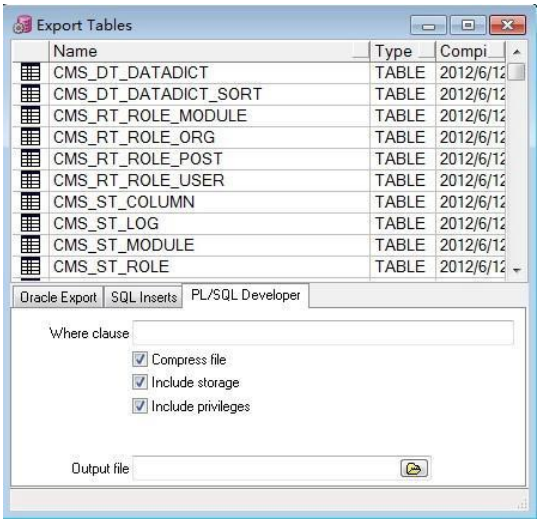
La exportación de datos sirve para mover datos de un entorno a otro. Por ejemplo, se pueden mover datos desde un entorno de desarrollo a uno de producción o desde una plataforma de base de datos a otra. Entre los diferentes tipos de métodos o aplicaciones se encuentran las siguientes:

PL/SQL DEVELOPER

Cláusula Where: habilite la operación de exportación para admitir la condición where. Por ejemplo, si solo necesita exportar 10,000 registros de cada tabla, puede ingresar "rownum <10001" en el cuadro de entrada. (Cómo hacer una copia de seguridad de la base de datos de Oracle con PL / SQL - programador clic, s. f.)

Comprimir archivo: después de seleccionar, admite la compresión de archivos exportados para ahorrar espacio de almacenamiento, pero la compresión tomará más tiempo. (Cómo hacer una copia de seguridad de la base de datos de Oracle con PL / SQL - programador clic, s. f.)

Incluir almacenamiento: el archivo exportado contiene información de creación de tablas. Si necesita admitir operaciones de creación de tablas durante la importación, debe seleccionar este elemento. (Cómo hacer una copia de seguridad de la base de datos de Oracle con PL / SQL - programador clic, s. f.)



1. EXPORTAR TABLAS. fuente: https://images4.programmerclick.com/785/96/96eb3170d7df98fa89d6b6dfb3175fa1.JPEG

Oracle – Exportación de Datos con Data Pump Import [impdp]

A partir de la versión 10g, Oracle incluye nuevas utilidades para importar y exportar datos mucho más potentes que los anteriores comandos imp y exp. (Marcos, 2015)

Hay que tener en cuenta que, aunque se trate de una evolución de la anterior herramienta de exportación exp, son comandos totalmente distintos. Si generamos la exportación con el comando exp, tendremos que emplear el comando imp y si la generamos con expdp, lo tendremos que importar con impdp. (Marcos, 2015)

b) Exportación de objetos

Un objeto de datos es una representación de datos basados en un archivo sin formato o tabla de base de datos relacional. Se puede importar un archivo sin formato o una tabla de base de datos relacional como objeto de datos físicos para usarlos como origen o destino en una asignación. (Resumen de la importación de objetos de datos físicos, s. f.)

Oracle Life Sciences Data Hub (Oracle LSH) (Exporting and Importing Objects, s. f.)

Dado que una secuencia de comandos SQL no puede referirse directamente a un directorio creado con el sistema operativo (SO), debe crear un directorio de base de datos local desde SQL*Plus y asignarlo al directorio del sistema operativo local.

La secuencia de comandos de exportación:

1. Registra todos los objetos que se exportan, con el comentario de registro "Registrado por IEU".
2. Crea un archivo comprimido con el nombre del Dominio como nombre de archivo (domain_name.zip). Este archivo contiene los metadatos de los objetos exportables contenidos en el Dominio.
3. Coloca el archivo de registro (domain_name.log) por separado en el mismo directorio

Exportación total y parcial

Cuando ejecuta el script de exportación, debe ingresar un valor de parámetro para indicar si desea realizar una exportación total o parcial.

Exportación completa . El script de exportación incluye automáticamente el Dominio que especifique y casi todos los objetos que contiene (consulte "Objetos incluidos" y "Objetos excluidos").

Exportación parcial . Debe llenar una tabla de controlador de base de datos con una lista de los objetos que se incluirán. El script incluye automáticamente los objetos contenidos en los objetos que especifique, incluidos los objetos contenidos en esos objetos y los objetos necesarios para que esos objetos existan.

Roles y privilegios necesarios para exportar

Cuando ejecuta el script, debe proporcionar una cuenta de usuario de Oracle LSH que tenga los siguientes privilegios:

Modifique los privilegios en todos los tipos de objetos que deben exportarse

El rol de la aplicación LSH Checkin Admin, si hay objetos en el Dominio que están desprotegidos por un usuario que no sea este usuario de la aplicación Oracle LSH

Estos privilegios son necesarios porque el script de exportación tiene que proteger todos los objetos extraídos antes de continuar con el resto del proceso de exportación.

Si el usuario de la aplicación no tiene privilegios suficientes y el script de exportación necesita registrar objetos, la exportación falla.

Creación del directorio y ejecución del script de exportación

Para ejecutar el proceso de exportación, haga lo siguiente desde el servidor de la base de datos donde tiene instalada la instancia de la base de datos de origen de Oracle LSH

1. Conéctese a la instancia de la base de datos como propietario del esquema de Oracle Applications; appspor lo general
2. Cree un directorio del sistema operativo donde desee que se genere la salida del script de exportación; por ejemplo, en el directorio principal del usuario de la aplicación Oracle LSH.
3. Asigne el directorio del sistema operativo a un directorio de base de datos utilizando el siguiente comando SQL:

CREATE DIRECTORY nombre_directorio_base_de_datos como ruta_del_directorio_SO

4. Desde el directorio del sistema operativo, ingrese el siguiente comando con los valores apropiados.
5. El script de exportación crea un archivo comprimido y un archivo de registro en el directorio de la base de datos. Ambos archivos tienen el nombre del dominio como nombre de archivo. Verifique el archivo .log de nombre_dominio para obtener detalles de la operación de exportación.

Importar objetos y datos.

a) Importación de datos

PL/SQL DEVELOPER

Eliminar tablas: admite la eliminación de tablas antes de importar datos. Después de seleccionar esta opción, la opción "Crear tablas" se selecciona de forma predeterminada, y las operaciones "Truncar tablas" y "Eliminar tabla" se vuelven grises y no están disponibles.

Crear tablas: Soporte para crear tablas antes de importar datos. Por ejemplo, hemos creado un usuario, y necesita importar tablas en este momento y no ha ejecutado el script de creación de tablas antes, puede seleccionar esta opción.

Truncar tablas: admite el borrado de datos de la tabla antes de importar los datos. Puede utilizar esta opción cuando desee restaurar los datos de la tabla al entorno de prueba. Esta opción es mutuamente excluyente con "Eliminar tablas".

Eliminar tablas: admite la eliminación de datos de tablas antes de importar datos. No se ha encontrado que esta opción tenga un significado especial. Esta opción y "Truncar tablas" son mutuamente excluyentes. La velocidad de importación de esta opción es mucho más lenta que la de "Truncar tablas", generalmente use "Truncar tablas".

Oracle – Importación de Datos con Data Pump Import [impdp]

Data Pump Import (en lo sucesivo, Importación para facilitar la lectura) es una utilidad para cargar un conjunto de archivos de volcado de exportación en un sistema de destino. El conjunto de archivos de volcado se compone de uno o más archivos de disco que contienen datos de tabla, metadatos de objetos de base de datos e información de control. Los archivos están escritos en un formato binario patentado. Durante una operación de importación, la utilidad Data Pump Import utiliza estos archivos para ubicar cada objeto de la base de datos en el conjunto de archivos de volcado. (Marcos, 2015)

La utilidad Importación de bomba de datos se invoca mediante el impdpcomando. Las características de la operación de importación están determinadas por los parámetros de importación que especifique. (Data Pump Import, s. f.)

b) Importación de objetos

Un objeto de datos es una representación de datos basados en un archivo sin formato o tabla de base de datos relacional. Se puede importar un archivo sin formato o una tabla de base de datos relacional como objeto de datos físicos para usarlos como origen o destino en una asignación.

Oracle Life Sciences Data Hub (Oracle LSH) (Exporting and Importing Objects, s. f.)

Dado que una secuencia de comandos SQL no puede referirse directamente a un directorio creado con el sistema operativo (SO), debe crear un directorio de base de datos local desde SQL*Plus y asignarlo al directorio del sistema operativo local.

El script de importación verifica si ya existe un Dominio con el mismo nombre que el Dominio que se está importando. Si lo hace, comprueba si el Dominio existente también se creó mediante el script de importación. Si el Dominio existente no es un Dominio importado, el script de importación crea un Dominio nuevo. Si el Dominio existente es un Dominio importado, actualiza los objetos que tienen nuevas versiones, lo que le permite implementar nuevas versiones de una aplicación Oracle LSH en la instancia de destino de Oracle LSH.

Actualización de un dominio existente

El script de importación realiza las siguientes tareas:

- Si algún objeto está actualmente desprotegido en el Dominio en la instancia de Oracle LSH de destino, el script los desprotege con el comentario "Registrado por IEU".
- Desprotege todos los objetos con el comentario "Desprotegido por IEU" y actualiza las versiones de las definiciones de objeto y las instancias si encuentra nuevas versiones en el archivo de exportación.
- Verifica las definiciones de objetos después de la creación de versiones y aplica el comentario "Registrado por IEU".
- Crea un archivo de registro en el directorio de la base de datos en la instancia de Oracle LSH de destino. El archivo de registro tiene el mismo nombre que el Dominio: nombre_dominio_import.log. Consulte "Importar contenido del archivo de registro" .
- Debe consultar el registro y decidir si desea o no realizar commit o cambios en la base de datos debido a la actualización. Puede rollback realizar los cambios si el registro de importación muestra problemas durante la actualización.

Roles y privilegios necesarios para importar dominios

Cuando ejecuta el script, debe proporcionar una cuenta de usuario de Oracle LSH que tenga los siguientes privilegios:

- Rol de aplicación LSH Checkin Admin . Este rol es esencial para importar o actualizar un Dominio.

- Rol de aplicación LSH Bootstrap Admin . Esta función solo se requiere para crear nuevos dominios, no para actualizaciones de dominios. Este rol permite que un usuario de la aplicación cree el Dominio y los objetos debajo de él.
- Privilegios suficientes para poder instalar Oracle LSH Work Areas.

Este usuario no requiere ningún otro privilegio para ejecutar la importación porque la seguridad del objeto se otorga temporalmente a este usuario como parte del proceso de importación.

Creación del directorio y ejecución del script de importación

Para importar un dominio LSH de Oracle, ejecute los siguientes comandos desde el servidor de la base de datos donde está instalada la instancia LSH de Oracle de destino:

1. Conéctese a la instancia de la base de datos como propietario del esquema de Oracle Applications; appspor lo general
2. Al menos la primera vez que ejecute el script, cree un directorio del sistema operativo donde desee que se genere el registro de importación. Por ejemplo, créelo en el directorio de inicio del usuario de la aplicación LSH para que sea fácil de encontrar.

   El proceso de importación crea un archivo .log que contiene información de metadatos del objeto LSH de Oracle que puede ser confidencial para su organización. Oracle recomienda otorgar acceso completo al directorio del sistema operativo solo al usuario de Oracle y al usuario que ejecuta el proceso de importación.

3. Asigne el directorio del sistema operativo a un directorio de base de datos utilizando el siguiente comando SQL:

   create directory <database_dir_name> as <path_of_the_OS_directory>

4. Vaya al directorio del sistema operativo que creó y copie el archivo de *dominio exportado en él.*
5. Ejecute el script de importación de la siguiente manera:

   sqlplus apps/< *contraseña_aplicaciones* >@< *LSH_target_database_server_name* > @< *ruta_de_cdrruimport.sql* > < *LSH_Application_Username* > < *Database_Directory_Name* > < *ZIP_Domain_Filename* > COMMIT_ON_NO_ERROR/MANUAL_COMMIT

6. El script de importación crea un archivo de registro en el directorio de la base de datos con un nombre en este formato: nombre_dominio_import.log.

Desarrollo de Base de Datos en la Web y el control de acceso.

La base de datos de un sitio web dinámico es aquel que contiene todos los datos necesarios para que el sitio funcione, es una parte esencial del sitio web. La base de datos en este caso debe contener datos administrativos como usuarios, permisos y contraseñas, así como datos textuales, que constituyen el contenido real del sitio, y otros datos que son esenciales para el funcionamiento de la empresa.

La base de datos de un sitio web tiene una variedad de utilidades, entre las que se incluye:

- La organización de datos de forma sencilla y fácil en un entorno colaborativo.
- Mantenimiento de bases de datos integradas a las herramientas de segmentación y envíos de comunicaciones.
- Control del flujo de información que pueden manejar a los usuarios a través de la visualización.
- Generar listas o reportes que puedan ser utilizados en las estrategias de comunicación de la empresa o en la emisión de resultados y medidas para tomar de decisiones.
- Llevar un control de las actividades realizadas en la base de datos a través del Log usado en Auditoría.
- Optimizar procesos de comunicación.

Beneficios

Se pueden clasificar en 4 grandes ventajas:

-Fácil de usar

Relacionado con lo amigable y lo intuitivo de las interfaces de la aplicación para realizar la carga de datos en las tablas de las bases de datos, el uso de las herramientas de búsquedas y segmentación, y la posibilidad de generar aplicaciones para acceder rápidamente a la información contenida en la misma base de datos.

-Configurable

Flexible y fácil para realizar las configuraciones y los cambios en las bases de datos, que permiten al usuario crear un campo nuevo en la base de datos, además de establecer relaciones entre varias bases de datos.

-Integrable

La integración del sistema de bases de datos se puede realizar tanto en sistemas externos como en módulos internos de la herramienta, a través de otros servicios web que son invisibles al usuario.

-Conectada

El manejo de la información involucra la unidad de registros de la Base de Datos, y la posibilidad de tener una revisión y consulta de los datos en tiempo real, debido a la capacidad de automatizar a sus plataformas de comunicación.

Características

- Se puede ordenar la información en campos y registros, dependiendo de lo que se necesite.
- Tiene la capacidad de hacer segmentaciones y otros cambios de la base de datos.
- Puede hacer búsquedas simples o avanzadas.
- Importa y exporta información desde y hacia otros programas aledaños a el web.
- Tiene indicadores gráficos y otros elementos que hacen más fácil el análisis de los datos para cualquiera.
- Da la alternativa de generar aplicaciones que faciliten el acceso a la base de datos.
- Crea grupos de visualización para restringir las vistas y la edición de campos específicos de una base de datos.
- Configura equipos de trabajo para controlar el acceso de otros usuarios a la información contenida en la base de datos.
- Configura tipos de datos para la generación de los campos en base a las necesidades de las empresas dueñas del sistema.

Control de acceso

Uno de los aspectos más relevantes de la seguridad de los datos es el control de acceso, el cual se encarga de brindar los permisos y accesos pertinentes a la información dentro de la empresa. Estos accesos se otorgan en base a las políticas de control de acceso, quienes dictan los niveles de acceso que van a tener los usuarios, para que estos tengan acceso apropiado a la información requerida.

Para llevar a cabo este control, se emplean diferentes metodologías de autenticación, las cuales pueden incluir credenciales, usuarios y contraseña, números PIN, seguridad biométrica, tokens de seguridad, etc. En vez de manejar los permisos de forma manual, las organizaciones con mayor seguridad dependen de soluciones de administración de identidad y acceso para implementar directivas de control de acceso.

Es importante mencionar que el control de acceso también es empleado para el acceso físico de la información en centros de datos, edificios, cuartos de seguridad, etc.

La premisa del control de acceso radica en saber quién es el usuario que quiere acceder a la información y a qué nivel de la información tiene acceso, lo que se busca con esto es que no todos los miembros de la empresa tengan acceso a toda la información, si no a la información especializada que requieren para llevar a cabo su labor dentro de la organización, también previene que usuarios infiltrados o no autorizados tengan acceso a esta información.

Las organizaciones eligen los métodos de autenticación de acuerdo con las necesidades de seguridad que requieran o dependiendo de las normas de seguridad establecidas para la información. Existen cuatro principales modelos de control de acceso:

1. Control de acceso discrecional (DAC)**:** en este método, el propietario o administrador del recurso, los datos o el sistema protegido establece las políticas de a quién se permite acceso.

2. Control de acceso obligatorio (MAC): en este modelo no discrecional, se garantiza a las personas el acceso basándose en una autorización de información. Una autoridad central regula los derechos de acceso basándose en distintos niveles de seguridad. Este modelo es común en entornos gubernamentales y militares.

3. Control de acceso basado en funciones (RBAC): RBAC concede acceso basándose en funciones empresariales definidas, en vez de la identidad del usuario individual. El objetivo es proporcionar a los usuarios acceso solo a datos que se hayan considerado necesarios para sus funciones en la organización. Este método de amplio uso se basa en una combinación compleja de asignaciones de funciones, autorizaciones y permisos.

4. Control de acceso basado en atributos (ABAC): en este método dinámico, el acceso se basa en un grupo de atributos y entornos medioambientales, como la hora del día y la ubicación, asignado tanto a usuarios como a recursos.

Uso de base de datos ORACLE como proveedor de servicios web

A través de paquetes PL/SQL y clases Java creadas dentro de la base de datos, Oracle Database puede conectarse a servicios web. La inversión en procedimientos almacenados de Java, paquetes PL/SQL, consultas SQL predefinidas y lenguaje de manipulación de datos (DML) se aprovecha al convertir Oracle Database en un proveedor de servicios web. En cambio, la integración de la información comercial es posible gracias al consumo de servicios web externos de la base de datos y la integración con el motor SQL.

Características de ORACLE como proveedor de servicios web

- **Mejorar los servicios web PL/SQL**

  Los servicios web de PL/SQL se han mejorado al agregar soporte para más tipos de PL/SQL, como CLOB, BLOB, XMLTYPE, cursor de referencia y tablas y registros de PL/SQL. La mayoría de sus paquetes PL/SQL actuales ahora se pueden usar como servicios web gracias a esto.

- **Exponer Java como servicios web en la base de datos.**

  Expone las clases de Java que ya están en Oracle Database como servicios web.

  Es posible mover clases de Java que implementan servicios relacionados con datos entre la base de datos y el nivel medio. La independencia de la base de datos es producida por la portabilidad de Java.

- **Activa los servicios web DML**

  Ofrece operaciones de registro, auditoría y rastreo que se implementan como servicios web utilizando DML cuadrado y son seguras, persistentes, transaccionales y escalables. Las operaciones atómicas, grupales o por lotes INSERTAR, ACTUALIZAR y ELIMINAR son la forma en que se implementan los servicios web DML.

Protección de los servicios web

- Cifrado, autenticación y autorización para servicios web mediante una arquitectura de seguridad integral basada en estándares.
- Los usuarios pueden gestionar de forma centralizada la seguridad del servicio web a través de un único punto de administración.

¿Qué sitios web utilizan la base de datos Oracle?

Dado que muchos clientes importantes utilizan Oracle Database como backend para sus aplicaciones web y todos quieren proteger la confidencialidad de la tecnología backend, no hay sitios web de buena reputación que revelen públicamente su tecnología. Sin embargo, se pueden reconocer los sitios creados con tecnologías de interfaz de usuario como Oracle Apex(es una herramienta de desarrollo rápido para aplicaciones web que se ejecutan en Oracle Database) y ADF(un marco Java con fines de lucro utilizado para crear aplicaciones comerciales).

Podemos mencionar los siguientes:

- www.netflix.com
- www.linkedin.com
- www.ebay.com
- www.nike.com
- www.jpmorganchase.com

- www.cisco.com

Oracle HTML DB ¿Qué es?

Oracle HTML BD permite la creación y el despliegue de aplicaciones web centradas en bases de datos a través de un entorno de desarrollo declarativo alojado.

Al permitir que varios grupos de trabajo desarrollen y usen aplicaciones como si estuvieran ejecutándose en diferentes bases de datos, transforma una única base de datos de Oracle en un servicio compartido. Oracle HTML DB acelera la creación de aplicaciones con sus funciones integradas, que incluyen temas de diseño, controles de navegación, controladores de formularios e informes flexibles.

Oracle HTML DB mantiene automáticamente el estado de la sesión sin necesidad de codificación. Oracle HTML DB administra el estado de la sesión en la base de datos de manera transparente para proporcionar un comportamiento con estado dentro de una aplicación. Las sustituciones simples y la sintaxis de la variable SQL están disponibles para los desarrolladores de aplicaciones para obtener y establecer el estado de la sesión.

El motor HTML DB utiliza los datos almacenados en las tablas de la base de datos para crear aplicaciones en tiempo real. Oracle HTML DB crea o modifica los metadatos que se almacenan en las tablas de la base de datos cuando crea o amplía su aplicación. El motor de la base de datos HTML lee los metadatos y representa la aplicación cuando se ejecuta.

Estas son las partes de la plataforma de desarrollo Oracle HTML DB.

- Desarrollador de aplicaciones
- Taller SQL.
- Taller de datos.

Refiriéndose al Desarrollador de aplicaciones

además de los objetos de la base de datos, como tablas y procedimientos, puede crear una interfaz (o aplicación) HTML utilizando Application Builder.

Un grupo de páginas web basadas en bases de datos conectadas por pestañas, botones o enlaces de hipertexto conforman una aplicación.

Utilizando las plantillas y los componentes de la interfaz de usuario que especifique, el motor de la base de datos HTML representa la aplicación después de crearla.

El bloque de construcción más fundamental de una aplicación es una página.

Cada página puede incluir lógica de aplicación (o procesos), botones, campos y más.

Puede usar la navegación condicional para moverse entre páginas, realizar cálculos, iniciar validaciones (como verificaciones de edición) y mostrar informes, formularios y gráficos.

Sobre Taller SQL

Accede a los objetos de la base de datos desde un navegador web usando SQL Workshop.

- Ejecuta scripts SQL después de cargarlos.
- Construir o modificar objetos de base de datos.
- Obtener más información sobre el diccionario de datos.
- La capacidad de profundizar y profundizar debe estar habilitada para la exploración de la base de datos.

Relacionado con el taller de datos

La base de datos alojada se puede utilizar para importar y exportar datos mediante Data Workshop. El texto (como datos delimitados por comas o tabuladores), los archivos XML y las hojas de cálculo son todos formatos de importación admitidos. El texto (incluidos los datos delimitados por comas o tabuladores) y los documentos XML son formatos de exportación admitidos.

Al usar el asistente de importación de hojas de cálculo, puede, por ejemplo, compartir datos rápidamente con numerosos usuarios al convertir una hoja de cálculo en una tabla de base de datos. Sin ningún conocimiento previo de SQL, el uso de este asistente crea una nueva tabla y carga los datos. Puede crear una aplicación sobre los datos una vez que se hayan cargado en una tabla de base de datos, tal como lo haría con cualquier otra tabla de base de datos.

La página de inicio de Oracle HTML DB aparece tan pronto como inicia sesión en el programa.

Hay tres partes en el entorno de desarrollo de Oracle HTML DB, como ya se mencionó anteriormente:

- Creador de aplicaciones(Aplication Builder)

Crea una interfaz (o aplicación) HTML sobre los objetos de la base de datos, como tablas y procedimientos, utilizando Application Builder.

- Taller de SQL(SQL Workshop)

Desde un navegador web, usa SQL Workshop para ver y administrar los objetos de la base de datos.

- Taller de datos(Data Workshop)

Para importar y exportar datos desde la base de datos alojada, use Data Workshop.

Acceso a datos con enlaces a bases de datos

Debido al hecho de que Oracle HTML DB se basa en una base de datos Oracle, puede utilizar todas las funciones de la base de datos distribuida.

Por lo general, los enlaces de bases de datos se utilizan para llevar a cabo operaciones de bases de datos distribuidas.

Debe crear un enlace de base de datos estándar utilizando la sintaxis de Oracle que se indica a continuación para poder utilizar enlaces de base de datos.

```
CREATE DATABASE LINK linkname
CONNECT TO username IDENTIFIED BY password
USING 'tns_connect_string';
```

La entrada `tns_connect_string` de su servidor local debe coincidir con los datos en sus SERVIDORES tnsnames.ora file Usar el nombre global de la base de datos remota como el nombre del enlace de su base de datos es una buena idea.

Controlar las preferencias del usuario

El estado de la sesión de un usuario se puede configurar mediante preferencias. Solo un administrador de Oracle HTML DB puede cambiar estas preferencias una vez que se han establecido. Las preferencias del usuario se pueden configurar mediante programación utilizando la API de PL/SQL, mediante la creación de un proceso de página o determinando el valor de origen del elemento de preferencia.

Se debe usar una API PL/SQL para establecer o hacer referencia a las preferencias del usuario mediante programación. El almacenamiento en caché a nivel de usuario habilitado mediante programación está disponible. Se puede establecer una preferencia a nivel de usuario con el nombre `NAMED_PREFERENCE` mediante la función `set_preferences`. Como se muestra a continuación:

```
HTMLDB_UTIL.SET_PREFERENCE(
```

```
 p_preference=>'NAMED_PREFERENCE',

 p_value =>v('ITEM_NAME'));
```

La función `GET_PREFERENCES` le permite referirse al valor de preferencia de un usuario.

Por ejemplo:

```
NVL(HTMLDB_UTIL.OBTENER_PREFERENCIA('NOMBRE_PREFERENCIA'),15)
```

Si la preferencia no tuviera valor, por defecto sería 15 en el ejemplo mencionado anteriormente.

Conclusiones

Equipo No. 1

Como observamos en la Investigación presentada anteriormente, el Manejo de Usuarios se convierte en un elemento primordial al momento no solamente del Diseño Conceptual o Lógico de una Base de Datos, sino que puede llegar a generar problemas en su desarrollo final, implementación y despliegue en servidores; lo que conllevaría a múltiples inconvenientes, que pueden ser traspasados casos de negocio en el que se ponga en riesgo la infraestructura crítica de la Empresa/Organización.

La minimización del riesgo a nivel de accesos de usuarios autorizados y no autorizados comienza directamente al momento en el que se establecen las conexiones iniciales a la Base de Datos, ya que hoy en día existen múltiples herramientas, como por ejemplo Identity Manager que han sido desarrolladas por la Unidad Funcional de Cloud en ORACLE, que permiten verificar ingresos no deseados o incluso intentos por fuerza bruta, que últimamente son los más comunes, incluyendo inyecciones SQL.

A continuación, presentamos las principales amenazas que existen para la integridad referencial y general de una Base de Datos como tal:

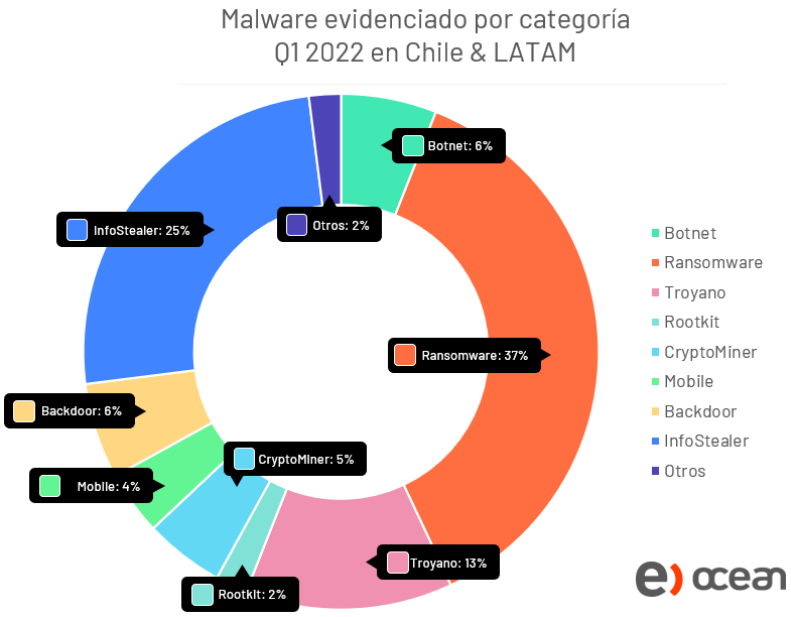


Figura N°3: Gráfico de Principales Amenazas en Q1 2022 (Fuente: ENTEL Ocean)

Se vuelve de vital importancia, que siendo ORACLE PL/SQL uno de los motores de Bases de Datos más utilizados para transacciones de alta redundancia por su reconocida fiabilidad e integridad en entornos empresariales; imperativo es el aseguramiento de ¿Quiénes tienen los accesos? ¿Quiénes tienen los permisos? ¿Cómo se tiene control acerca de lo que ve el usuario final o no, que es por ello

que una buena prática es la de evitar que se vea cualquier tipo de código, sino que todo lo requerido por las Unidades Funcionales del Negocio, se muestre a través de una “Vista”.

Equipo No. 2

El tema de administración de privilegios y funciones de base de datos son de los casos de prioridad más sensitivos e importantes en una empresa u organización, dichos privilegios determinan el modus operandi en términos de jerarquías de sistemas de información que establecen todo el flujo de transacciones e información del cual todo la organización depende, si se necesita revisar, modificar, o simplemente tener acceso a dicho sistema de base de datos, la importancia del establecimiento de privilegios, aumenta y hace posible la seguridad del sistema de cualquier, inconveniente no deseado; desde errores humanos hasta de intrusiones de actores no deseados con intensiones o no, al sistema permitiendo su funcionamiento optimo; dicho esto; se puede concluir; por cada herramienta de sistema que permita el control y la asignación de roles, privilegios y sus funciones, da más opciones de generar un sistema de base de datos más seguro, eficiente y funcional para cualquier tipo de casos de uso y usuarios, adaptable para cualquier necesidad profesional e incluso personal, pero también para mantener su objetivo principal, la información de estos; consistente.

Equipo No. 3

La cuota es el espacio que el usuario podrá utilizar en el sistema, de no ser asignado por defecto será cero, por lo que dicho usuario no podrá crear nada. Se pueden asignar cuotas por usuarios o grupo de usuario y según la capacidad de definir cuotas en los distintos niveles brindará un control sobre el almacenamiento disponible.

Los perfiles son fundamentales para controlar el comportamiento del usuario y el uso que les da a los recursos de la base de datos. El utilizarlos es de suma importancia para mantener una buena seguridad de la base de datos y aumentar el rendimiento de la misma, disminuyendo el uso de recursos innecesarios de esta y del sistema.

Equipo No. 4

Verificar la identidad de los usuarios es de suma importancia en distintos ámbitos y las Bases de Datos no son la excepción. Que cada persona cuente con su propio nombre de usuario y contraseña nos permitirá establecer niveles de seguridad y a su vez mantener un orden en el acceso a la base de datos.

A través de esta gestión de usuarios podemos considerar los distintos permisos, que pueden ser privilegios o restricciones, que tendrá cada usuario al interactuar con la base de datos.

Para esta investigación nos centramos en el Software de Bases de Datos Oracle en donde se vio a detalle elementos como el perfil de usuario predeterminado, sus funciones, etc.

A su vez se detallaron variables de perfil con sus respectivos comandos o sintaxis en donde posteriormente a la creación del usuario se establecen los limites de uso de recurso de la base de datos.

Equipo No. 5

A manera de conclusión podemos decir que el respaldo nos es de gran importancia, ya que nos permite prevenir la perdida de información, y para lograr ello PL/SQL nos brinda diferentes opciones; lograr la importación y exportación de datos, así como también de objetos, se logra disponiendo de diferentes comandos, la aplicación de los mismos nos asegura que ante cualquier desastre de índole física (como inundaciones en el centro de datos, fluctuaciones de electricidad que pueda dañar el equipo, fuego, entre otros), y de índole informática, es decir daños en el mismo software en sí (introducción de malware que pueda borrar o hacer cambios en la información), cualquier tipo de amenaza interna o externa que represente una amenaza para la integridad de los datos y la estructura que contiene la misma, sea respaldada en otro servidor como un plan B ante cualquier inconveniente.

Equipo No. 6

Utilizar Oracle Database tiene la libertad de almacenar sus datos como quiera, la capacidad de acceder a ellos rápidamente y la fuerza para mantenerlos seguros.

Se puede usar una variedad de funciones PL/SQL para habilitar su base de datos en la web y hacer que sus datos administrativos sean interactivos y estén disponibles para los usuarios de la intranet o sus clientes.

Uno de los sistemas de administración de bases de datos más potentes de la industria es Oracle. Es un sistema comercial utilizado a nivel mundial con fuertes características comerciales.

En Oracle HTML DB, los servicios web se basan en el estándar SOAP (Protocolo simple de acceso a objetos). El World Wide Web Consortium (W3C) ha establecido SOAP como un protocolo estándar para transferir solicitudes y respuestas a través de Internet. Un proveedor de servicios y un usuario de servicios pueden enviar y recibir mensajes SOAP utilizando sobres SOAP.

Los sobres SOAP con formato XML incluyen una solicitud para una acción específica, así como el resultado de esa acción.Las funciones principales de una base de datos son responder consultas y realizar transacciones de datos, y la forma más popular de hacerlo en la actualidad es integrándola en páginas web.

Dependiendo de los requisitos de seguridad que tengan o de los estándares de seguridad establecidos para la información, las organizaciones eligen los métodos de autenticación.

Bibliografía

- "Oracle autonomous database en infraestructura de exadata dedicada". Oracle Help Center. https://docs.oracle.com/es-ww/iaas/autonomous-database/doc/managing-database-users.html (accedido el 9 de noviembre de 2022).
- H. Paredes. "Usuario SYS y SYSTEM - ORACLE". Blog | hadsonpar. http://blog.hadsonpar.com/2016/02/usuario-sys-y-system-oracle.html (accedido el 9 de noviembre de 2022).
- "Diseño de seguridad de una base de datos". Universidad de Don Bosco, El Salvador. https://www.udb.edu.sv/udb_files/recursos_guias/informatica-ingenieria/base-de-datos-i/2019/i/guia-12.pdf (accedido el 8 de noviembre de 2022).
- "Seguridad de datos: En qué consiste y qué es importante en tu empresa". PowerData - Especialista en Gestión de Datos | MDM | Big Data | Cloud | Data Warehouse. https://www.powerdata.es/seguridad-de-datos (accedido el 9 de noviembre de 2022).
- "Desbloqueo de cuentas de usuario (guãa del administrador de negocio de sun identity manager 8.1)". Moved. https://docs.oracle.com/cd/E19957-01/821-0062/byaee/index.html (accedido el 10 de noviembre de 2022).
- "Usuarios bloqueados en Oracle". Informaticadas. http://informaticadasdecadadia.blogspot.com/2014/02/usuarios-bloqueados-en-oracle.html (accedido el 10 de noviembre de 2022).
- *Jorge Sánchez. Manual de Administración de Bases de Datos. Administración de usuarios en Oracle Database*. (s. f.). https://jorgesanchez.net/manuales/abd/control-usuarios-oracle.html
- *¿QUE ES UN PRIVILEGIO EN ORACLE?* (2014, 9 diciembre). BLOG: Administración de Base de Datos. https://blogjosearcosc.wordpress.com/que-es-un-privilegio-en-oracle/
- *Uso de privilegios (tareas) - Administración de Oracle Solaris 11.1: servicios de seguridad*. (2014, 1 enero). https://docs.oracle.com/cd/E37929_01/html/E36668/privtask-1.html
- Olvera, V. T. L. E. D. O. O. (2013, 2 agosto). *Manejo de perfiles*. Orlando Olguín Olvera. https://orlandoolguin.wordpress.com/2009/09/20/manejo-de-perfiles/
- Gestión de seguridad en Oracle I. (2009, 8 enero). Desarrollo Web. https://desarrolloweb.com/articulos/gestion-seguridad-oracle-I.html
- Turmero, P. (2021, 12 marzo). Bases de datos Oracle (página 2). Monografias.com. https://www.monografias.com/trabajos106/bases-datos-oracle/bases-datos-oracle2

- *Sanchez, J. (s. f.). Jorge Sánchez. Manual de Administración de Bases de Datos. Administración de usuarios en Oracle Database. JorgeSanchez.net. Recuperado 9 de noviembre de 2022, de https://jorgesanchez.net/manuales/abd/control-usuarios-oracle.html*
- *Cómo modificar el perfil predeterminado y Límite PASSWORD_VERIFY_FUNCTION / Seabrookewindows.com. (2022, 26 enero). seabrookewindows.com. https://www.seabrookewindows.com/BQq292JMK/*

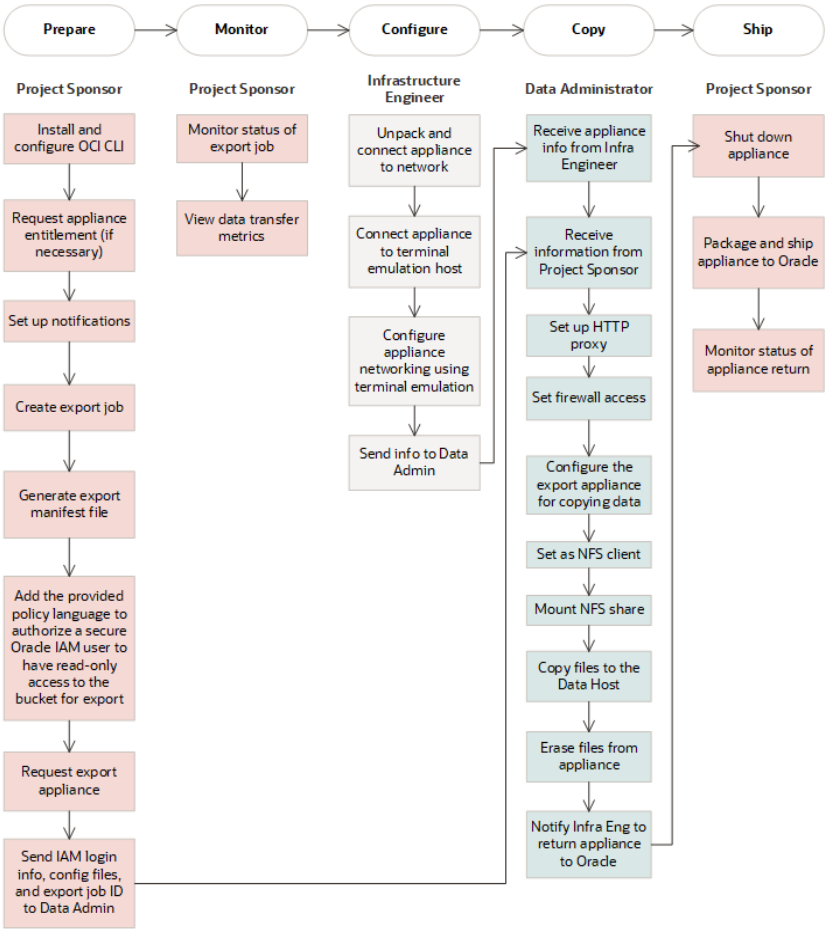
- *Cómo hacer una copia de seguridad de la base de datos de Oracle con PL / SQL - programador clic*. (s. f.). https://programmerclick.com/article/55461369804/
- *Data Pump Import*. (s. f.). https://docs.oracle.com/cd/B19306_01/server.102/b14215/dp_import.htm
- *Exportar tablas PLSQL DEVELOPER*. (s. f.). programmerclick. https://images4.programmerclick.com/785/96/96eb3170d7df98fa89d6b6dfb3175fa1.JPEG
- *Exporting and Importing Objects*. (s. f.). https://docs.oracle.com/cd/E18315_02/doc.214/e18305/export.htm
- *Importar y exportar datos*. (s. f.). https://help.highbond.com/helpdocs/analytics/142/scripting-guide/es/Content/lang_ref/commands/import_and_export_data.htm
- *1 What is Oracle HTML DB?* (s. f.). https://docs.oracle.com/cd/B14117_01/appdev.101/b10992/mvl_intro.htm
- *Base de Datos Web*. (2012, 16 febrero). Modelos de BD. https://modelosbd2012t1.wordpress.com/2012/02/16/base-de-datos-web/
- *Creación de sitios web: Sistemas de bases de datos*. (s. f.). GCFGlobal.org. https://edu.gcfglobal.org/es/creacion-de-sitios-web/sistemas-de-bases-de-datos/1/
- *Database Web Services*. (s. f.). https://docs.oracle.com/database/121/JJDEV/chtwelve.htm
- *Developing Web Applications with PL/SQL*. (s. f.). https://docs.oracle.com/cd/A97630_01/appdev.920/a96590/adgweb.htm
- Microsoft. (s. f.). *¿Qué es el control de acceso?* | *Seguridad de*. https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control
- *Oracle Application Server Web Services*. (s. f.). https://docs.oracle.com/cd/B14099_19/web.1012/b14027/orawebservices.htm
- Thomson Data. (2022, 29 agosto). *Companies That Use Oracle - Oracle Customers List*. https://www.thomsondata.com/customer-base/oracle.php

Anexos

Exportación de Datos - Oracle Cloud Infrastructure (Preparación para la exportación de datos, s. f.)

La exportación de datos la podemos definir como una solución de exportación de datos fuera de línea de Oracle que le permite migrar juegos de datos a escala de petabyte desde el cubo de Object Storage de Oracle Cloud Infrastructure a su centro de datos mediante un dispositivo de transferencia de datos proporcionado por Oracle. Hay que tener en cuenta que no puede exportar datos de varios cubos de Object Storage al mismo trabajo de exportación. Si desea exportar datos de más de un cubo, debe crear un trabajo de exportación para cada uno de los cubos.

A continuación, se muestra una visión general de alto nivel de las tareas implicadas en la exportación de datos desde Oracle Cloud Infrastructure al centro de datos:



2. Exportación de datos desde Oracle Cloud Infrastructure. fuente:https://docs.oracle.com/en-us/iaas/Content/Resources/Images/breadcrumb_export_prepare.png

Ahora a continuación mencionaré los pasos para realizar dicha tarea de exportación de datos:

Para exportar datos a un archivo:

1. Haga clic en Aplicación y, a continuación, haga clic en Descripción general.
2. Haga clic en Acciones y, a continuación, Exportar datos.
3. Haga clic en Crear.
4. En la página Exportar datos, seleccione el entorno de destino del archivo de exportación de datos:

*Local: guarda el archivo de exportación de datos en una ubicación del equipo local.

*Buzón de salida: Guarda el archivo de exportación de datos en el servidor. Consulte Carga y descarga de archivos utilizando el explorador de bandeja de entrada/buzón de salida.

5. Seleccione el Cubo
6. Seleccione el tipo de archivo:

*Delimitado por comas: crea un archivo .csv delimitado por comas para cada artefacto.

*Delimitado por tabuladores: Crea un archivo .txt delimitado por tabuladores para cada artefacto.

*Otro: Crea un archivo .txt para cada artefacto. Introduzca el carácter delimitador que desea utilizar en el archivo de exportación. Para obtener una lista de los caracteres delimitadores y las excepciones admitidos, consulte Otros caracteres delimitadores soportados.

7. En Listas inteligentes, especifique Exportar etiquetas o Exportar nombres.
8. Para los miembros dinámicos, seleccione si desea incluir o excluir los miembros de cálculo dinámico durante la exportación.
9. Para los Decimales, especifique el número de decimales (0-16) para formatear los datos tras la exportación, o bien seleccione la opción predeterminada, Ninguno, para usar el formato de precisión predeterminado. Por ejemplo, especificar un valor decimal de 3 en el campo Decimales hará que los datos exportados muestren tres dígitos a la derecha de la coma decimal, cuando sea aplicable.
10. Seleccione el segmento de datos que se va a exportar.
11. Opcional: haga clic en Guardar como trabajo para guardar la operación de exportación como un trabajo, el cual puede programar para que se ejecute inmediata o posteriormente.
12. Haga clic en Exportar y, a continuación, especifique una ubicación para guardar el archivo de exportación de datos.

Importación de Objetos – Analytics (Importar y exportar datos, s. f.)

Comandos para la importación de datos	
Accessdata	Importa datos de una variedad de orígenes de datos compatibles con ODBC. El comando toma la forma de ACCESSDATA64 o ACCESSDATA32; todo

	depende de si usted está usando un controlador ODBC de 64 bits o de 32 bits.
Import access	Crea una tabla de Analytics definiendo e importando un archivo de base de datos Microsoft Access.
Import delimited	Crea una tabla de Analytics definiendo e importando un archivo de texto delimitado.
Import excel	Crea una tabla de Analytics definiendo e importando un intervalo con nombre o una hoja de cálculo de Microsoft Excel.
Import grcproject	Crea una tabla de Analytics importando una tabla de Proyectos de HighBond.
Import grcresults	Crea una tabla de Analytics importando una tabla o interpretación de Resultados de HighBond.
Import multidelimited	Crea varias tablas de Analytics definiendo e importando varios archivos delimitados.
Import multiexcel	Crea varias tablas de Analytics definiendo e importando varios intervalos con nombre u hojas de cálculo de Microsoft Excel.
Import odbc	Crea una tabla de Analytics definiendo e importando datos desde un origen de datos ODBC. ODBC significa Open Database Connectivity (Conectividad de base de datos abierta), un método estándar para acceder a bases de datos.
Import pdf	Crea una tabla de Analytics definiendo e importando un archivo de Adobe PDF.
Import print	Crea una tabla de Analytics definiendo e importando un archivo de imagen de impresión (reporte).
Import sap	Crea una tabla de Analytics importando datos desde un sistema SAP utilizando Direct Link.
Import xbrl	Crea una tabla de Analytics definiendo e importando un archivo XBRL.

Import xml

Crea una tabla de Analytics definiendo e importando un archivo XML.

Retrieve

Recupera los resultados de una consulta de Direct Link enviada para su procesamiento en segundo plano.