Administración de Bases de Datos

Configuración y Administración del espacio en disco

Privilegios y Usuarios en Oracle

Crear Usuarios y asignar privilegios en Oracle

El siguiente es un resumen de algunas consideraciones al momento de crear un usuario o cuenta en Oracle, y los privilegios y roles que se le pueden asignar.

- El nombre de usuario no debe superar los 30 caracteres, no debe contener caracteres especiales y debe iniciar con una letra.
- Debe contar con un método de autentificación. El más común es la contraseña, pero existen otros métodos como los datos biometricos, el uso de certificados y autentificación por medio de un token.
- Asignar un Tablespace por default, donde el usuario va a poder crear sus objetos si no se indica otra cosa. Esto no significa que automáticamente pueda crear objetos, o que tenga una cuota de espacio, debido a que son permisos que se asignan de forma separada. Si utiliza el privilegio RESOURCE, se le asigna una quota unlimited, incluso en el Tablespace SYSTEM. Si esto ocurre, se deberán mover los objetos creados en SYSTEM a otro Tablespace.
- Asignar un Tablespace temporal, donde el usuario para los objetos temporales que se requieren en indexación, ordenamientos, etc.
- Asignar un perfil de usuario, si requiere de indicar las restricciones especiales que debe tener su cuenta, como limitar el uso de recursos y reforzar las reglas de seguridad a nivel de cuentas, lo que es recomendable en ambientes de Desarrollo

Ejemplo

```
SQL> CREATE USER jperez IDENTIFIED BY juper DEFAULT TABLESPACE
users TEMPORARY TABLESPACE temp PROFILE perfil_desarrollo;
```

Modificar cuentas de Usuarios

Hay diversas alternativas para modificar un usuario creado, por ejemplo, si se debe cambiar su contraseña, su tablespace por omisión, su tablespace temporal, su quota o su perfil:

```
SQL> ALTER USER NOMBRE_USUARIO IDENTIFIED BY CLAVE_ACCESO [DEFAULT
TABLESPACE ESPACIO_TABLA] [TEMPORARY TABLESPACE ESPACIO_TABLA]
[QUOTA {ENTERO {K | M } | UNLIMITED } ON ESPACIO_TABLA [PROFILE
```

```
PERFIL];
```

Privilegios de Sistema y de Objetos

En Oracle existen dos tipos de privilegios de usuario.

- **Privilegios de Sistema:** Son los que permiten al usuario hacer ciertas tareas sobre la Base de Datos, 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.

  En general los privilegios de sistema, permiten ejecutar comandos del tipo DDL (Data definition Language), como CREATE, ALTER y DROP o del tipo DML (Data Manipulation Language). Estos privilegios de sistema pueden ser consultados en la vista: SYSTEM_PRIVILEGE_MAP.

  Entre todos los privilegios de sistema que existen, hay dos que son muy importantes: SYSDBA y SYSOPER. Estos son dados a los usuarios con funciones de administración de la base de datos.

  Se pueden otorgar varios permisos a la vez, por ejemplo:

  ```
  SQL> GRANT CREATE USER, ALTER USER, DROP USER TO ahernandez;
  ```

- **Privilegios de Objetos:** Este tipo de permiso le permite al usuario realizar ciertas acciones en objetos de la Base de Datos, tales como una Tabla, una Vista, un Procedimiento o una Función. 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 el dueño del objeto, el administrador o alguien que haya recibido este permiso explícitamente y tenga Grant Option. Por ejemplo:

  ```
  SQL> GRANT SELECT,INSERT,UPDATE,DELETE ON analista.venta TO
  jperez;
  ```

  Adicionalmente, se pueden restringir los privilegios DML a una columna de la tabla mencionada.

  Si se desea que este usuario pueda dar permisos sobre la tabla venta a otros usuarios, se emplea la cláusula WITH GRANT OPTION:

  ```
  SQL> GRANT SELECT,INSERT,UPDATE,DELETE ON analista.venta TO
  mgarcia WITH GRANT OPTION;
  ```

Asignar cuotas a Usuarios

Por defecto ningún usuario tiene cuota en los Tablespaces, se tienen tres opciones para poder asignar una quota a un usuario:

- **Unlimited**, que permite al usuario usar todo el espacio disponible de un Tablespace.

  Por medio de un valor determinado, que puede ser en kilobytes o megabytes que el usuario puede usar. Este valor puede ser mayor o menor que el tamaño

del Tablespace asignado a él.

Por medio del privilegio UNLIMITED TABLESPACE, que tiene prioridad sobre cualquier cuota asignada en un Tablespace y por lo tanto, se tiene disponibilidad de todo el espacio incluyendo en los tablespaces de SYSTEM y SYSAUX.

No se recomienda dar cuotas a los usuarios en los Tablespaces SYSTEM y SYSAUX, sólo los usuarios SYS y SYSTEM pueden crear objetos en estos tablespaces. Tampoco se deben dar cuotas en los Tablespaces Temporal o del tipo Undo.

Roles

Los Roles son simplemente un conjunto de privilegios que se pueden otorgar a un usuario o a otro Rol. De esa forma se simplifica el trabajo del DBA en esta tarea.

Por default cuando creamos un usuario desde el Enterprise Manager se le asigna el permiso de connect, lo que permite al usuario conectarse a la Base de Datos y crear sus propios objetos en su propio esquema. De otra manera, habría que asignarlo en forma manual.

Para crear un Rol se hace de la siguiente manera:

```
SQL> CREATE ROLE appl_dba;
```

Para asignar este Rol a un usuario:

```
SQL> GRANT appl_dba TO jperez;
```

Otro uso común de los roles es asignarles privilegios a nivel de Objetos, por ejemplo en una Tabla de Facturas en donde sólo se puedan hacer consultas e inserciones:

```
SQL> CREATE ROLE consulta;
SQL> GRANT SELECT,INSERT on analista.factura TO consulta;
```

Y luego se asigna ese rol a distintos usuarios finales:

```
SQL> GRANT consulta TO ahernandez;
```

En Oracle existen algunos roles predefinidos, tales como:

```
CONNECT, CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE
SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK, CREATE CLUSTER,
ALTER SESSION, RESOURCE, CREATE PROCEDURE, CREATE SEQUENCE, CREATE
TRIGGER, CREATE TYPE, CREATE CLUSTER, CREATE INDEXTYPE, CREATE
OPERATOR SCHEDULER, CREATE ANY JOB, CREATE JOB, EXECUTE ANY CLASS,
EXECUTE ANY PROGRAM, MANAGE SCHEDULER, etc.
```

DBA: Tiene la mayoría de los privilegios, no es recomendable asignarlo a usuarios que no son administradores.

SELECT_CATALOG_ROLE: No tiene privilegios de sistema, pero tiene cerca de 1600 privilegios de objeto.

Para consultar los roles definidos y los privilegios otorgados a través de ellos, utilice las siguientes vistas:

```
SQL> select * from DBA_ROLES;
SQL> select * from DBA_ROLE_PRIVS order by GRANTEE;
```

Roles fijos de nivel de servidor en SQL Server

- **Sysadmin.** Los miembros del rol fijo de servidor sysadmin pueden realizar cualquier actividad en el servidor.
- **Serveradmin.** Los miembros del rol fijo de servidor serveradmin pueden cambiar opciones de configuración en el servidor y cerrar el servidor.
- **Securityadmin.** Los miembros del rol fijo de servidor securityadmin administran los inicios de sesión y sus propiedades.

  Pueden administrar los permisos de nivel de servidor GRANT, DENY, y REVOKE.

  También pueden administrar los permisos de nivel de base de datos GRANT, DENY y REVOKE si tienen acceso a una base de datos.

  Además, pueden restablecer las contraseñas de los inicios de sesión en SQL Server.

  IMPORTANTE: La capacidad de conceder acceso al motor de base de datos y configurar los permisos de usuario permite que el administrador de seguridad asigne la mayoría de los permisos de servidor.

  El rol securityadmin se debe tratar como equivalente al rol sysadmin.

  Como alternativa, a partir de SQL Server 2022 (16.x), considere la posibilidad de usar el nuevo rol fijo de servidor ##MS_LoginManager##.
- **Processadmin.** Los miembros del rol fijo de servidor processadmin pueden finalizar los procesos que se ejecutan en una instancia de SQL Server.
- **Setupadmin.** Los miembros del rol fijo de servidor setupadmin pueden agregar y quitar servidores vinculados mediante instrucciones Transact-SQL. (para usar Management Studio es necesario ser administrador del sistema).
- **Bulkadmin.** Los miembros del rol fijo de servidor bulkadmin pueden ejecutar la instrucción BULK INSERT.

  El rol bulkadmin o los permisos ADMINISTER BULK OPERATIONS no son compatibles con SQL Server en Linux. Solo sysadmin puede realizar inserciones masivas para SQL Server en Linux.
- **Diskadmin.** El rol fijo de servidor diskadmin se usa para administrar archivos de disco.
- **Dbcreator.** Los miembros del rol fijo de servidor dbcreator pueden crear, modificar, quitar y restaurar cualquier base de datos.
- **Public.** Cada inicio de sesión de SQL Server pertenece al rol del servidor público.

  Cuando a una entidad de seguridad de servidor no se le han concedido ni

denegado permisos específicos para un objeto protegible, el usuario hereda los permisos concedidos al rol público en ese objeto.

Solo asigne los permisos públicos en cualquier objeto cuando desee que el objeto esté disponible para todos los usuarios. No se puede cambiar de miembro en público.

Nota: El rol public se implementa de manera diferente que otros roles y los permisos se pueden conceder, denegar o revocar de los roles fijos de servidor públicos.

Roles fijos adicionales a nivel de servidor

- **##MS_DatabaseConnector##.** Los miembros del rol fijo de servidor **##MS_DatabaseConnector##** pueden conectarse a cualquier base de datos sin necesidad de que una cuenta de usuario de la base de datos se conecte. Para denegar el permiso **CONNECT** a una base de datos específica, los usuarios pueden crear una cuenta de usuario coincidente para este inicio de sesión en la base de datos y, a continuación, **DENY** al permiso **CONNECT** al usuario de base de datos. Este permiso **DENY** anulará el permiso **GRANT CONNECT** procedente de este rol.
- **##MS_LoginManager##.** Los miembros del rol fijo del servidor **##MS_LoginManager##** pueden crear, eliminar y modificar inicios de sesión. A diferencia del antiguo rol fijo del servidor **securityadmin**, este rol no otorga privilegios GRANT a sus miembros. Es un rol más limitado que ayuda a cumplir con el *Principio del privilegio mínimo*.
- **##MS_DatabaseManager##.** Los miembros del rol fijo de servidor **##MS_DatabaseManager##** pueden crear y eliminar bases de datos. Un miembro del rol **##MS_DatabaseManager##** que crea una base de datos se convierte en el propietario de dicha base de datos, lo que permite que el usuario se conecte a ella como el usuario dbo. El usuario dbo tiene todos los permisos de base de datos en la base de datos. Los miembros del rol **##MS_DatabaseManager##** no necesariamente tienen permiso para acceder a las bases de datos que no son de su propiedad. Este rol del servidor tiene los mismos privilegios que el rol dbcreator en SQL Server, pero recomendamos usar este nuevo rol en lugar del anterior, ya que este rol existe también en Azure SQL Database y por lo tanto ayuda a usar los mismos scripts en diferentes ambientes.
- **##MS_ServerStateManager##.** Los miembros del rol fijo de servidor **##MS_ServerStateManager##** tienen los mismos permisos que el rol **##MS_ServerStateReader###.** Además, contiene el permiso **ALTER SERVER STATE**, que permite el acceso a varias operaciones de administración, como DBCC FREEPROCCACHE, DBCC FREESYSTEMCACHE ('ALL') y DBCC SQLPERF()
- **##MS_ServerStateReader##.** Los miembros del rol fijo de servidor

##MS_ServerStateReader## pueden leer todas las vistas de administración dinámica (DMV) y funciones que están incluidas en **VIEW SERVER STATE**, y respectivamente tiene permiso **VIEW DATABASE STATE** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario.

- **##MS_ServerPerformanceStateReader##.** Los miembros del rol fijo de servidor **##MS_ServerPerformanceStateReader##** pueden leer todas las vistas de administración dinámica (DMV) y las funciones cubiertas por **VIEW SERVER PERFORMANCE STATE**, respectivamente tiene permiso **VIEW DATABASE PERFORMANCE STATE** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario. Se trata de un subconjunto al que tiene acceso el rol del servidor **##MS_ServerStateReader##**, lo que ayuda a cumplir con el *Principio de privilegio mínimo*.
- **##MS_ServerSecurityStateReader##.** Los miembros del rol fijo de servidor **##MS_ServerSecurityStateReader##** pueden leer todas las vistas de administración dinámica (DMV) y las funciones cubiertas por **VIEW SERVER SECURITY STATE**, y respectivamente tiene permiso **VIEW DATABASE SECURITY STATE** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario. Se trata de un subconjunto al que tiene acceso el rol del servidor **##MS_ServerStateReader##**, lo que ayuda a cumplir con el *Principio de privilegio mínimo*.
- **##MS_DefinitionReader##.** Los miembros del rol fijo del servidor **##MS_DefinitionReader##** pueden leer todas las vistas de catálogo cubiertas por **VIEW ANY DEFINITION**, y respectivamente tienen permiso **VIEW DEFINITION** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario.
- **##MS_PerformanceDefinitionReader##.** Los miembros del rol fijo del servidor **##MS_PerformanceDefinitionReader##** pueden leer todas las vistas de catálogo cubiertas por **VIEW ANY PERFORMANCE DEFINITION**, y respectivamente tienen permiso **VIEW PERFORMANCE DEFINITION** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario. Se trata de un subconjunto al que tiene acceso el rol del servidor **##MS_DefinitionReader##**.
- **##MS_SecurityDefinitionReader##.** Los miembros del rol fijo de servidor **##MS_SecurityDefinitionReader##** pueden leer todas las vistas de catálogo cubiertas por **VIEW ANY SECURITY DEFINITION**, y respectivamente tiene el permiso **VIEW SECURITY DEFINITION** en cualquier base de datos en la que el miembro de este rol tenga una cuenta de usuario. Este es un pequeño subconjunto de lo que el rol del servidor **##MS_DefinitionReader##** tiene acceso, lo que ayuda a cumplir con el *Principio de privilegio mínimo*.