# Schema Only Accounts - Oracle Database 18c

Por Francisco Riccio

## Introducción

A partir de la versión Oracle Database 18c, es posible crear schemas que no puedan autenticarse dentro de la base datos debido a que carecen de algún tipo de autentificación definido (password, externa o global).

En el desarrollo de aplicaciones, todos los objetos (tablas, índices, programas PL/SQL, etc.) desplegados pertenecen a un schema, el cual tiene un método de autenticación y por ende es utilizado en la cadena de conexión hacia la base de datos en la gran mayoría de casos. Hoy esto puede ser eliminado al no tener una autenticación, obligando a los desarrolladores a crear un usuario específicamente para la cadena de conexión de la aplicación y asignarle los privilegios correctos a los objetos que requieran ser accedidos.

Existen algunas consideraciones a tener presente:

- Dentro de una instancia +ASM no pueden crearse schema only accounts.
- Puede asignarse cualquier privilegio de objeto, sistema y roles; a excepción de: SYSDBA, SYSOPER, SYSBACKUP, SYSKM, SYSASM, SYSRAC y SYSDG.
- Restringido a ser conectado vía un DBLINK.
- Disponible para base de datos CDB y NOCDB.

Esta nueva funcionalidad también es utilizada por Oracle para proveer algunos de sus esquemas internos.

## Implementación

### A. Creación del Schema Only Account

Sintaxis: CREATE USER <nombre_usuario> NO AUTHENTICATION

Ejemplo:

```
SQL> create user friccio no authentication;

User created.
```

Validamos en la vista DBA_USERS la creación del schema only account:

```
SQL> select USERNAME,AUTHENTICATION_TYPE
     from dba_users where username='FRICCIO';

USERNAME             AUTHENTICATION_TYPE
-------------------- ------------------------
FRICCIO              NONE
```

## B. Asignación de Privilegios y Creación de Objetos

La asignación de privilegios y creación de objetos es como tradicionalmente se ha venido trabajando en versiones anteriores, ejemplo:

```
SQL> grant resource to FRICCIO;

Grant succeeded.

SQL> create table FRICCIO.Producto (cod number, nombre varchar(20));

Table created.

SQL> alter table FRICCIO.Producto add constraint PK_Producto primary key(cod);

Table altered.

SQL> create view FRICCIO.VProducto as select * from FRICCIO.Producto;

View created.

SQL> create or replace procedure FRICCIO.SPU_Producto is begin null; end;
/

Procedure created.
```

Se valida la creación de los objetos:

```
SQL> select object_name, object_type
     from dba_objects where owner='FRICCIO';

OBJECT_NAME          OBJECT_TYPE
-------------------- -----------------------
PRODUCTO             TABLE
PK_PRODUCTO          INDEX
VPRODUCTO            VIEW
SPU_PRODUCTO         PROCEDURE
```

Una vez creado el schema only account el cual es el owner de los objetos de negocio, debe crearse un diseño de seguridad para asignar los correctos privilegios a los usuarios que serán utilizados en la cadena de conexión de las aplicaciones.

Como en todas las versiones de base de datos Oracle, también es posible cambiar el actual schema que tenemos, ejemplo:

```
SQL> show user
USER is "SYS"
SQL> ALTER SESSION SET CURRENT_SCHEMA=FRICCIO;

Session altered.

SQL> select * from vproducto;

no rows selected
```

## C. Proxy Authenticated Connection

Es posible realizar una conexión a la base de datos a través de Proxy Authenticated Connection mediante un usuario y tener la sesión del Schema Only Account. Esto nos permite crear objetos de manera más sencilla y es una opción más completa que el ejemplo anterior.

Ejemplo:

```
SQL> create user proxy_friccio identified by oracle;

User created.

SQL> grant connect to proxy_friccio;

Grant succeeded.

SQL> alter user friccio grant connect through proxy_friccio;

User altered.

SQL> connect proxy_friccio[friccio]/oracle
Connected.
SQL> column "session" format a20
SQL> column "session_schema" format a25
SQL> column "proxy_user" format a20
SQL> select sys_context('USERENV','SESSION_USER') as "session",
     sys_context('USERENV','SESSION_SCHEMA') as "session_schema",
     sys_context('USERENV','PROXY_USER') as "proxy_user"
     from dual;

session              session_schema            proxy_user
-------------------- ------------------------- --------------------
FRICCIO              FRICCIO                   PROXY_FRICCIO

SQL> show USER
USER is "FRICCIO"
```

**D. Conversión de Schema a Schema Only Account y Viceversa.**

Se puede realizar cualquier conversión a través de la sentencia: ALTER USER.

Es importante recordar que si la conversión será hacia Schema Only Account se debe cumplir las consideraciones previamente presentadas. Ejemplo:

```
SQL> create user demo identified by oracle;

User created.

SQL> alter user demo no authentication;

User altered.

SQL> alter user demo identified by oracle;

User altered.
```

Sobre el mismo ejemplo, si no cumplimos con las consideraciones presentadas se conseguirá el siguiente error:

```
SQL> grant sysdba to demo;

Grant succeeded.

SQL> alter user demo no authentication;
alter user demo no authentication
*
ERROR at line 1:
ORA-40367: An Administrative user cannot be altered to have no authentication
type.
```

En caso se desee realizar la conversión debe retirársele al usuario todos los privilegios no permitidos.

## Conclusión

Esta nueva funcionalidad que nos provee Oracle Database 18c permite crear schemas sin autenticación reforzando nuestros niveles de seguridad en la base de datos al no permitir que las aplicaciones utilicen el usuario (dueño de los objetos de negocio) en la cadena de conexión o manipular los objetos directamente desde alguna herramienta.

**Publicado por:**

**Francisco Riccio,** actualmente se desempeña como Arquitecto de Soluciones en Oracle Perú y es instructor de cursos oficiales de certificación Oracle. Es un Oracle Certified Professional en productos de Oracle Application, Base de Datos, Cloud & Virtualización.