**ADMINISTRACIÓN Y AUTENTIFICACIÓN DE USUARIOS**

Todo acceso a una base de datos requiere conectar mediante un usuario y contraseña. Dicho usuario dará derecho a utilizar ciertos objetos de la base de datos, pero tendrá restringido (salvo que se trate de un superadministrador) el uso de otros.

A los usuarios se les asigna una serie de privilegios que son los que dan permiso de uso a ciertos objetos. Estos privilegios suelen agruparse en lo que se conoce como roles, que permiten estructurar mejor los permisos que se conceden a los usuarios. El perfil del usuario será el conjunto de permisos y restricciones que se aplican a dicho usuario.

Por ello cuando un usuario conecta debe probar que es quien dice ser (normalmente mediante una contraseña), es decir se autentifica. Por otro lado esta autentificación dará lugar a unos privilegios (unos derechos) y unas restricciones.

**Creación de Usuarios**

Una de las más básicas tareas de un administrador de base de datos es identificar los usuarios. Cada usuario que conecta en la base de datos debe de tener una cuenta. En las cuentas compartidas son difíciles de aplicar una auditoria.

Para crear un usuario utilizamos la sentencia **CREATE USER**. Cuando creas una cuenta como mínimo tienes que asignar un único nombre (username) y una contraseña para poder autenticarse.

Para cambiar alguno de los atributos que se le ha añadido al usuario creado se utiliza la sentencia **ALTER USER**.

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

* **Nombre de usuario**. 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 (**\_**). Además el nombre no puede comenzar con un número.
* **Configuración física**. Se refiere al espacio asociado al usuario para almacenar sus datos (lo que Oracle llama **tablespace**) y la cuota (límite de almacenamiento) que se le asigna a dicho usuario y mediante la que se establece el espacio máximo que el usuario puede gastar en el tablespace.
* **Perfil asociado**. El perfil del 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. El bloqueo lo realiza el DBA:
  + **ALTER USER** usuario **ACCOUNT LOCK**
  + **Expirada**. La cuenta agotó el tiempo máximo asignado a ella. Para salir de este estado, el usuario/a debe resetear su contraseña de usuario.
  + **Expirada y bloqueada**.
  + **Expirada en periodo de gracia**. Está en los últimos momentos de uso antes de pasar a estado de expirada.

**Autenticación Oracle**

Cuando uno se conecta con una instancia de una base de datos la cuenta de usuario debe de estar autenticada. ORACLE provee tres métodos de autenticación para nuestra cuenta de usuario.

* **Autenticación mediante password**

Cuando un usuario conecta con una base de datos verifica que este usuario y la contraseña introducida almacenada en la base de datos, sea correcta. Las contraseñas se guardan encriptadas en la base de datos (en el data dictionary).



* **Autenticación externa**

Cuando un usuario conecta con la base de datos se verifica que el nombre de usuario es el mismo que el nombre de usuario del sistema operativo para permitir la validación.

No se almacenan las cuentas en la base de datos de ninguna forma. Estas cuentas están siempre referidas con OPS$. A partir de la versión 10g puedes configurar **OS\_AUTHENT\_PREFIX** en el spfile.



Mediante **IDENTIFIED EXTERNALLY** decimos a la base de datos que nuestra cuenta es externa y tiene que ser validada con el sistema operativo.

* **Autenticación global**

Cuando un usuario se conecta con la base de datos se verifica globalmente cuando la información pasa por una opción avanzada de seguridad (**ADVANCED SECURITY OPTION**) para la autenticación tal como Kerberos, RADIUS …

Para las cuentas globales no se almacena tampoco nada en la base de datos.



Mediante **IDENTIFIED GLOBALLY** decimos a la base de datos que nuestra cuenta se autentica globalmente, mediante otra opción de seguridad avanzada.

**Borrado De Un Usuario**

Para borrar un usuario utilizamos la sentencia **DROP USER**, podemos opcionalmente incluir la opción **CASCADE**, se utiliza para borrar recursivamente los objetos del usuario que se pretende borrar.



**Cuentas de usuario bloqueadas y no bloqueadas**

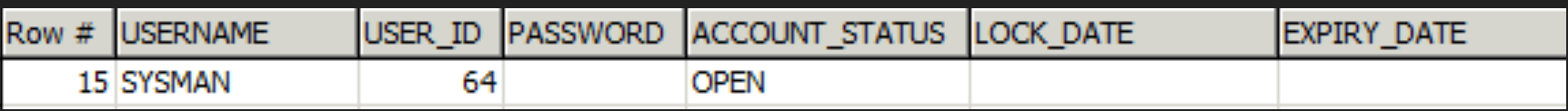
**Cuentas bloqueadas por límite de intentos de inicio de sesión**

Si se está trabajando con una aplicación vinculada a una base de datos y utilizando las capacidades de esta, si tiene soporte para gestionar usuarios, es posible encontrarse con el problema de que un usuario llegue al máximo número de intentos de inicio de sesión y que, en consecuencia, se bloquee su cuenta.

En Oracle para ver la lista de los usuarios que se tienen y sus diferentes propiedades, como si está bloqueado o no, se ejecuta este comando en el editor de SQL:

**SQL**> **SELECT** \* **FROM** dba\_users;

Este comando permitirá observar una tabla como la siguiente, con la información de todos los usuarios que se encuentren en la base de datos:



Cuando uno de estos usuarios llega al máximo número de intentos de acceso y se bloquea, se actualizan el ACCOUNT\_STATUS y el LOCK\_DATE, y por ende, el usuario no podrá entrar a la aplicación.

Los usuarios que tienen bloqueado el acceso a la interfaz de olvido de contraseña debido a un exceso de intentos fallidos de inicio de sesión no pueden iniciar la sesión en dicha interfaz hasta que un administrador desbloquee la cuenta, hasta que el usuario bloqueado (o un usuario con capacidades adecuadas) cambie o reinicialice la contraseña del usuario), o hasta que caduque el bloqueo.

Si se define un valor de tiempo de espera de bloqueo en la directiva de cuentas de *Identity Manager* [1], el bloqueo de una cuenta acabará caducando.

**Cuentas bloqueadas por administrador de base de datos**

Para denegar temporalmente el acceso a la base de datos a una cuenta de usuario en particular, es posible bloquear la cuenta de usuario. Si el usuario intenta conectarse, la base de datos muestra un mensaje de error y no permite la conexión. En este caso, es posible desbloquear la cuenta de usuario cuando se desee volver a permitir el acceso a la base de datos para ese usuario.

Para bloquear una cuenta de usuario se utiliza el siguiente comando:

**SQL**> **ALTER** **USER** username **ACCOUNT** **LOCK**;

Un administrador puede desbloquear una cuenta si tiene control administrativo sobre la organización a la que está afiliado el usuario y posee la capacidad *Desbloquear usuario*.

Un administrador con capacidades adecuadas puede aplicar las operaciones siguientes al estado de bloqueo de un usuario.

* Actualizar (incluido el reabastecimiento de recursos)
* Cambiar o reinicializar la contraseña
* Inhabilitar o habilitar
* Renombrar
* Desbloquear

**Para desbloquear un usuario**

Mediante la tabla **dba\_users** podemos ver los usuarios bloqueados filtrando por los que el **atributo lock\_date no sea null:**



Una vez identificado el usuario bloqueado, lo podremos desbloquear mediante **account unlock**:



Podemos ver como el **account\_status** cambia de “**LOCKED(TIMED)**” a “**OPEN**“:



**Usuarios expirados**

Por defecto, en ORACLE 11g, si los usuarios se crean bajo el ROLE Default, estarán sujetos a una política en la cual la contraseña caducará a los 180 días.

Esto es bueno puesto que te obliga a cambiar la contraseña. El problema es cuando uno desconoce esta política o se le olvida cambiar la contraseña en ese tiempo y el usuario, pasado ese periodo, se bloquea con sus correspondientes consecuencias para la aplicación que lo usa.

Para poder ver si en nuestra base de datos tenemos activa esta política ejecutamos la siguiente consulta:



El resultado que obtenemos en este caso el siguiente:



Si queremos verificar a qué profile está asociado nuestro usuario, lo podemos hacer con la siguiente consulta:



Para cambiar esta política en el ROLE DEFAULT y establecerla a indefinida permitiéndonos así a nosotros cambiar la contraseña del usuario cuando creamos conveniente ejecutaremos la siguiente consulta:



En caso de que nuestro usuario haya sido bloqueado debido a que ya pasaron los 180 días desde su creación o cambio de contraseña, podremos desbloquearlo y cambiar la contraseña de la siguiente forma:



**Usuarios predeterminados de la Base de Datos**

|  |  |  |
| --- | --- | --- |
| **USUARIOS PREDETERMINADOS** | | |
| **Usuario** | **Contraseña** | **Propósito** |
| SYS | CHANGE\_ON\_INSTALL INTERNAL | Usuario utilizada para realizar tareas de administración de la base de datos. |
| SYSTEM | MANAGER | Otro usuario utilizada para realizar tareas de administración de bases de datos. |
| ANONYMOUS | ANONYMOUS | Habilita el acceso HTTP a Oracle XML DB. |
| APEX\_PUBLIC\_USER |  | Es un usuario con privilegios mínimos utilizada para la configuración de Oracle Application Express con Oracle Application Express Listener o Oracle HTTP Server y mod\_plsql. |
| FLOWS\_FILES |  | Es el usuario propietario de los archivos cargados de Oracle Application Express. |
| APEX\_040000 |  | Es el usuario que posee el esquema y los metadatos de Oracle Application Express. |
| OUTLN | OUTLN | Usuario que respalda la estabilidad del plan. La estabilidad del plan le permite mantener los mismos planes de ejecución para las mismas sentencias SQL. OUTLN actúa como una función para administrar de forma centralizada los metadatos asociados con los esquemas almacenados. |
| DIP | DIP | Usuario genérico DIP para procesar eventos propagados por DIP. Esta cuenta sería utilizada por todas las aplicaciones que utilizan el servicio de aprovisionamiento DIP al conectarse a la base de datos. |
| ORACLE\_OCM | ORACLE\_OCM | Este usuario contiene la instrumentación para la recopilación de configuraciones que usa Oracle Configuration Manager. |
| XS$NULL |  | Es un usuario interno que representa la ausencia de un usuario en una sesión. Dado que XS $ NULL no es un usuario, solo la instancia de Oracle Database puede acceder a esta cuenta. |
| MDSYS | MDSYS | Es el usuario administrador de Oracle Spatial and Graph y Oracle Multimedia Locator. |
| CTXSYS | CTXSYS | Es el usuario utilizado para administrar Oracle Text. Oracle Text le permite crear aplicaciones de consulta de texto y aplicaciones de clasificación de documentos. Proporciona indexación, búsqueda de palabras y temas, y capacidades de visualización de texto. |
| DBSNMP | DBSNMP | Es el usuario utilizada por el componente de Agente de administración de Oracle Enterprise Manager para monitorear y administrar la base de datos. |
| XDB | CHANGE\_ON\_INSTALL | Usuario utilizada para almacenar datos y metadatos de Oracle XML DB. Oracle XML DB proporciona almacenamiento y recuperación XML de alto rendimiento para datos de Oracle Database. |
| APPQOSSYS |  | Usuario utilizado para almacenar y administrar todos los datos y metadatos requeridos por Oracle Quality of Service Management. |
| HR | HR | Usuario propietario del esquema de recursos humanos incluido en los esquemas de muestra de Oracle. |

**REFERENCIAS BIBLIOGRÁFICAS**

[1] J. Sánchez. (s.f.). *Administración de usuarios en Oracle Database.* JorgeSanchez.net.Sitio web: https://jorgesanchez.net/manuales/abd/control-usuarios-oracle.html

[2] Informe ejecutivo de Oracle. (junio 2008). *Introducción a Oracle Identity Management.* Oracle. Sitio web: https://www.oracle.com/technetwork/es/documentation/317540-esa.pdf

[3] Oracle Corporation. (2010). *Desbloqueo de cuentas de usuario.* Oracle. Sitio web: https://docs.oracle.com/cd/E19957-01/821-0062/byaee/index.html

[4] Informaticadas. (febrero 2014). *Usuarios bloqueados en Oracle.* Sitio web: http://informaticadasdecadadia.blogspot.com/2014/02/usuarios-bloqueados-en-oracle.html

[5] Oracle Help Center. (s.f.). *Locking and Unlocking User Accounts.* Oracle. Sitio web: https://docs.oracle.com/database/121/ADMQS/GUID-6A8D4A59-6DB2-4662-BA4C-05B914D31B4F.htm#ADMQS12042

[6] Oracle. (s.f.). *Oracle9i Default Accounts and Passwords.* Sitio web: https://docs.oracle.com/cd/A97630\_01/win.920/a95490/username.htm

[7] Oracle Help Center. (s.f.). *Oracle Database System Privileges Accounts and Passwords.* Oracle. Sitio web: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/hpdbi/oracle-database-system-privileges-accounts-and-passwords.html#GUID-7513171C-1055-48BB-8C79-B27EECC9B7E9

[8] Oracle Help Center. (s.f.). *Database 2 Day + Security Guide.* Oracle. Sitio web: https://docs.oracle.com/cd/E11882\_01/server.112/e10575/tdpsg\_user\_accounts.htm#TDPSG20000

[9] Admin. (diciembre, 2010). Administración de Usuarios en Oracle. Sitio web: https://orasite.com/tutoriales/administracion/administracion-de-usuarios-en-oracle

[10] Admin. (marzo, 2014). ORA-28001: la contraseña ha expirado. Sitio web: https://orasite.com/tutoriales/administracion/contrasena-expirado-expired-password

[11] Systemadmin. (octubre, 2013). Desbloquear usuario en ORACLE. Sitio web: http://systemadmin.es/2013/10/desbloquear-usuario-en-oracle