Tema 9

Seguridad.

Introducción a la seguridad de bases de datos

- Oracle utiliza los esquemas y dominios de seguridad para controlar el acceso a los datos y restringir el uso de los recursos de diferentes bases de datos.

- Oracle proporciona un control de acceso discrecional.

- El control de acceso discrecional regula con privilegios todo el acceso del usuario a los objetos.

- Un privilegio es un permiso para acceder a un objeto con nombre en la forma prevista, por ejemplo, el permiso para consultar una tabla.

Los usuarios de las bases de datos y esquemas

- Cada base de datos Oracle tiene una lista de nombres de usuario.

- Para acceder a una base de datos, el usuario debe usar una aplicación de base de datos e intentar realizar una conexión con un nombre de usuario de la base de datos.

- Cada nombre de usuario tiene una contraseña asociada para prevenir el uso no autorizado.

Los usuarios de las bases de datos y esquemas

- Cada usuario tiene un dominio de seguridad:
  - Conjunto de propiedades de seguridad que determinan aspectos tales como:
    - Las acciones que se le permiten llevar a cabo (privilegios y roles).
    - Las cuotas de espacio del usuario en los diferentes tablespaces (espacio disponible en los discos).
    - Límites a los recursos del sistema (por ejemplo, tiempo de proceso de la CPU).
- Un privilegio es el derecho de ejecutar un determinado tipo de sentencia SQL.

Tablespace por defecto

- Cuando un usuario crea un objeto del esquema (tabla, índice ó cluster) y no especifica un tablespace para contenerlo, entonces:
  - Se utiliza el tablespace por defecto del usuario.
  - Además ha de tener:
    - Privilegio para crear el objeto de esquema.
    - Cuota disponible en el tablespace.

Tablas temporales

- Cuando un usuario ejecuta una instrucción SQL que requiere la creación de segmentos temporales (tal como la creación de un índice), se utiliza el tablespace temporal del usuario.

- Al situar los segmentos temporales de todos los usuarios en un tablespace dedicado, se puede reducir el flujo de E/S entre los segmentos temporales y otros tipos de segmentos.

Cuotas de tablespace

- Oracle puede limitar la cantidad total de espacio en disco disponible para todos los objetos de un esquema.

- Esto permite controlar la cantidad de espacio en disco que puede ser consumido por los objetos de cada esquema.

Cifrado de datos transparente

- Oracle proporciona seguridad mediante:
  - Autentificación
    - Garantiza que sólo accedan al sistema aquellos usuarios que estén autorizados.
  - Autorización
    - Asegura de que los usuarios sólo tengan acceso a los recursos a los que se les ha permitido acceder.
  - Auditoría
    - Garantiza la rendición de cuentas cuando los usuarios acceden a los recursos protegidos.

Cifrado de datos transparente

- A pesar de estos mecanismos de seguridad que protegen eficazmente los datos en la base de datos, no se impide el acceso a los archivos del sistema operativo donde se almacenan los datos.

- Oracle permite el cifrado de los datos que se almacenan en los archivos del sistema operativo.

- Además, se puede aplicar un módulo de seguridad, externo a la base de datos, para el almacenamiento y gestión segura de las claves.

Métodos de autentificación

- Autentificación:
  - Verificar la identidad de alguien.

- Oracle requiere de procedimientos especiales de autentificación para los administradores de bases de datos, porque realizan operaciones especiales de bases de datos.

- Oracle también cifra las contraseñas durante la transmisión de información para garantizar la seguridad de autentificación de red.

Métodos de autentificación

- Atendiendo a:
  - Quién lleva a cabo la autentificación:
    - Por el sistema operativo.
    - Por la red.
    - Por la base de datos Oracle.
    - Por parte del protocolo Secure Socket Layer.
  - A qué afecta la autentificación:
    - Autentificación y autorización multicapa.
    - De administradores de bases de datos.

Autentificación por parte del sistema operativo

- Algunos sistemas operativos permiten utilizar a Oracle la información que mantienen de los usuarios para llevar a cabo su autentificación.

Autentificación por la Red

- Oracle soporta los siguientes métodos de autentificación por la red:
  - De terceros, basadas en las tecnologías de autentificación.
  - De clave pública, basada en las infraestructuras de autentificación.
  - Autentificación remota.

Autentificación por la base de datos Oracle

- Oracle ofrece un conjunto de ayudas a la autentificación de los usuarios:
  - Cifrado de contraseñas.
  - Bloqueo de cuenta.
  - Tiempo de vida y caducidad de las contraseñas.
  - Verificación de complejidad de las contraseñas.

Autentificación por parte del protocolo Secure Socket Layer

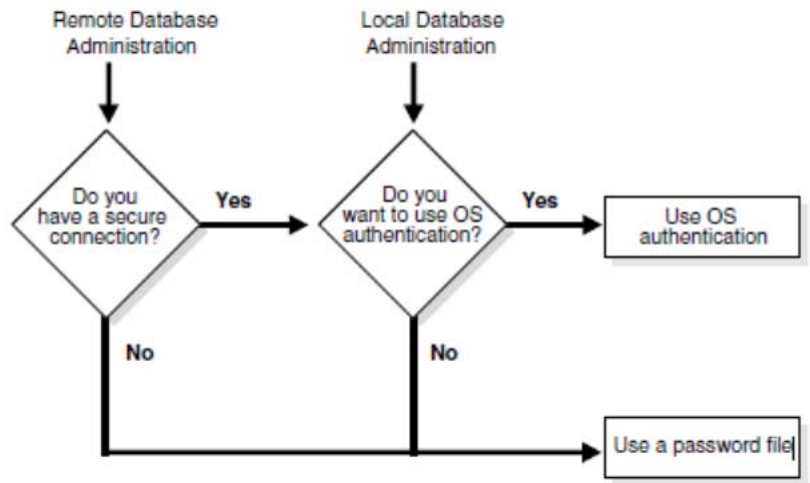
- El protocolo Secure Socket Layer (SSL) es un protocolo de la capa de aplicación.

- Los usuarios que se identifican de manera externa o global, pueden autentificarse en una base de datos a través del protocolo SSL.

Autentificación de administradores de bases de datos

•Los administradores de base de datos realizan operaciones especiales y se puede elegir entre la autenticación por el sistema operativo o mantener archivos de contraseñas para autentificarlos.

Figure 20–1 Database Administrator Authentication Methods



Descripción general de la autorización

- La autorización incluye principalmente dos procesos:
  - Permitir sólo a determinados usuarios acceder, procesar, o alterar los datos.
  - Establecer limitaciones diferentes sobre el acceso de los usuarios o acciones.
    - Las limitaciones impuestas a los usuarios pueden aplicarse a:
      - Los objetos, tales como esquemas, tablas o filas.
      - A los recursos, tales como el tiempo (CPU, conectar, o los tiempos de inactividad).

Limites y recursos del sistema

- Como parte del dominio de seguridad del usuario, pueden ponerse límites al uso de los recursos disponibles del sistema.

- La manera de administrarlos es a través del perfil del usuario, que es un conjunto nominado de límites sobre los recursos que se le pueden asignar.

- El administrador de seguridad puede habilitar ó inhabilitar los perfiles.

Los recursos del sistema y sus límites

- A cada usuario se le asigna un perfil, que especifica las limitaciones sobre los recursos disponibles del sistema.

- Incluyendo:
  - El número de sesiones concurrentes que el usuario puede establecer.
  - El tiempo de cpu.
  - Cantidad de I/O.
  - La cantidad de tiempo ocioso permitido.
  - La cantidad de tiempo de conexión permitido.
  - Restricciones en las claves.
  - Bloqueo de la cuenta después de una determinada cantidad de intentos de conexión fallidos.
  - Expiración de las claves y período de gracia.
  - Reutilización de claves y restricciones.

Perfiles

- Un perfil es un conjunto nominado de límites específicos de uso o asignación de recursos de una base de datos ORACLE.

- Para usar perfiles se deben tipificar los tipos de usuario de la base de datos.

- Antes de crear los perfiles y asignarle los limites en el uso o asignación de recursos, se deben determinar los valores apropiados.

- Para ello se puede recolectar la información acerca del uso de los recursos.

- ORACLE provee diversas herramientas y opciones para conseguir la información necesaria acerca del uso de los recursos por parte de los diferentes perfiles de usuarios.

Roles

- En general se emplean para asignar los privilegios relacionados con los usuarios finales de las aplicaciones de un sistema o para asignar roles a otro roles.

- Los roles de la base de datos tienen la siguiente funcionalidad:
  - Un rol puede tener privilegios del sistema y privilegios de objetos del esquema.
  - Un rol se puede asignar a otro roles (excepto a si mismo directa o indirectamente).
  - A cualquier usuario de la base de datos se le puede asignar cualquier rol.
  - Un rol asignado a un usuario se puede habilitar o inhabilitar en cualquier momento.

Descripción general de la auditoría de base de datos

- La Política de Auditoria.
  - Los administradores de Seguridad deben establecer una política para el procedimiento de auditoria de cada base de datos.
  - Cuando es necesaria una auditoria el administrador de seguridad debe decidir a que nivel de detalle se realizará la auditoría de la base de datos.
  - Una vez detectada alguna actividad de origen sospechosa a través del sistema general de auditoria, se realizará una auditoría más especifica.

Política de Seguridad de la Información

- La seguridad de datos incluye los mecanismos que controlan el acceso y el uso de la base de datos en el nivel de objeto.

- Su política de seguridad de datos determina qué usuarios tienen acceso a objetos de esquema específicos, y los tipos específicos de acciones permitidos para cada usuario sobre el objeto.

- También debería definir las acciones, para cualquiera, que sea auditado para cada objeto de esquema.

Seguridad por contraseña

- Si la autentificación de usuarios es administrada por la base de datos, los administradores de seguridad deberían desarrollar una política de seguridad por contraseña para mantener la seguridad de acceso a la base de datos.

- Para proteger mejor la confidencialidad de su contraseña, Oracle puede configurarse para emplear contraseñas encriptadas en conexiones cliente/servidor y servidor/servidor.

Administración de privilegios

- Los administradores de seguridad deben considerar los temas relacionados a la administración de privilegios para todos los tipos de usuarios.

- Los administradores de seguridad que administran una base de datos con muchos usuarios, aplicaciones u objetos deberían aprovecharse de los beneficios que ofrece en empleo de roles.

- Los roles simplifican en gran medida la tarea de la administración de privilegios en entornos complejos.

Seguridad de Usuario Final

- Los administradores de seguridad deben definir también una política para la seguridad de usuario final.

- Si una base de datos es grande y con muchos usuarios, el administrador de seguridad puede:
  - Decidir que grupos de usuarios pueden ser categorizados.
  - Crear roles de usuarios para esos grupos de usuarios.
  - Otorgar los privilegios necesarios o roles de aplicación para cada rol de usuario.
  - Asignar los roles de usuarios a los usuarios.

Administrador de Seguridad

- Los administradores de seguridad deben tener una política de seguridad.

- Los roles administrativos pueden otorgarse a los usuarios administradores apropiados.

- Por otro lado, cuando la base de datos es pequeña y tiene pocos administradores puede ser más conveniente crear un rol administrativo y otorgarlo a todos los administradores.

Seguridad de Desarrollador de Aplicaciones

- Los administradores de seguridad deben definir una política especial de seguridad para los desarrolladores de aplicaciones que usen bases de datos.

- Un administrador de seguridad solo debe otorgar privilegios, los necesarios para crear los objetos que necesiten los desarrolladores, a los administradores de bases de datos, y ellos se encargarán de recibir los pedidos de creación de objetos por parte de los desarrolladores.

Seguridad de Administrador de Aplicaciones

- En grandes sistemas de bases de datos con muchas aplicaciones (por ejemplo, precompiladores y aplicaciones de formularios) podría existir un administrador de aplicaciones.

- Éste sería responsable de las siguientes tareas:
  - Creación de roles para aplicaciones y manejo de privilegios para cada rol de las aplicaciones.
  - Creación y manejo de objetos usados por una aplicación en la base de datos.
  - Mantenimiento y actualización del código de las aplicaciones y de los procedimientos de Oracle.