MECANISMOS DE SEGURIDAD

Integrantes:
-> Christian Jimbo
-> Jairo González
-> Jorge Sarmiento

Seguridad de datos

Oracle ofrece:

- CIFRADO Y ALMACENAMIENTO
    - Oracle Advanced Security ofrece un cifrado transparente de los datos almacenados y de los datos en tránsito.
    - Oracle Secure Backup es una solución de backup en cinta que cifra las bases de datos y los datos del sistema de archivos.
    - Oracle Data Masking des-identifica los datos de producción antes de transferirlos a entornos de prueba o a socios.
- CIFRADO TRANSPARENTE DE DATOS (TDE):
    - Permite cifrar datos confidenciales tales como números de tarjetas de crédito almacenados en tablas y espacios de tabla. Los datos cifrados se descifran de forma transparente para una aplicación o un usuario de base de datos que tenga acceso a los datos. TDE ayuda a proteger los datos almacenados en medios en caso de sustracción de los medios de almacenamiento o los archivos de datos. Oracle usa mecanismos de autenticación, autorización y auditoría para proteger los datos de la base de datos, pero no los archivos de datos del sistema operativo donde se almacenan datos. Para proteger estos archivos de datos, Oracle proporciona TDE. TDE cifra los datos confidenciales almacenados en los archivos de datos. Para evitar descifrados no autorizados, TDE almacena las claves de cifrado en un módulo de seguridad externo a la base de datos.

      Aplicación de creación de cartera

      Se crea la carpeta de cartera.

      ```
      mkdir C:\oracle\admin\wallets
      OEM > login as sys / sysdba
      OEM > Server > Transparent Data Encryption
      Advanced Options > Change Location
           Host Credentials    Username: <DOMAIN>\dbs_ora
      Password: xxxxxxx
           Configuration Method: File System
      Encryption Wallet Directory: C:\oracle\admin\wallets
           OK
      Create Wallet > Local Auto-Open Wallet > Create
      ```

```
     Host Credentials    Username: <DOMAIN>\dbs_ora
Password: xxxxxxx
     Wallet Password:  walletadmin
     Continue
```

Se realiza una copia de seguridad de la carpeta de cartera.

```
cd C:\oracle\admin
zip -r wallets wallets
```

En la ventana de comando, se crea la carpeta de cartera.

```
mkdir C:\oracle\admin\wallets
```

Se agrega la ubicación de cartera al archivo sqlnet.ora.

```
ENCRYPTION_WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)    (METHOD_DATA =

      (DIRECTORY =
C:\oracle\admin\wallets\$ORACLE_SID)
```

Se genera una clave principal

```
alter system set encryption key identified by
"walletadmin";
```

/*Nota*/ Se debe comprobar el estado de la cartera

```
select * from "v$encryption_wallet";
```

Se establece la cartera para inicio de sesión automático

```
set ORACLE_SID=revdb
orapki wallet create -wallet C:\oracle\admin\wallets
-auto_login -pwd walletadmin
```

Se crea una copia de la cartera

```
cd C:\oracle\admin
zip -r wallets wallets
```

Control de usuarios

Asignación de atributos de seguridad a los usuarios en Trusted Extensions

El rol de administrador de la seguridad asigna los atributos de seguridad a los usuarios en Solaris Management Console una vez que se crean las cuentas de usuario. Si estableció los valores predeterminados correctos, el siguiente paso consiste en asignar los atributos de seguridad únicamente a los usuarios que necesiten excepciones a los valores predeterminados.

Al asignar los atributos de seguridad a los usuarios, el administrador de la seguridad considera la siguiente información:

Asignación de contraseñas

El rol de administrador de la seguridad asigna contraseñas a las cuentas de usuario una vez que se crean las cuentas. Después de esta asignación inicial, los usuarios pueden cambiar sus contraseñas.

Como en el SO Oracle Solaris, se puede obligar a los usuarios a que cambien sus contraseñas periódicamente. Las opciones de caducidad de las contraseñas limitan el período durante el que un intruso capaz de adivinar o robar la contraseña puede acceder al sistema. Además, al establecer que transcurra un período mínimo antes de poder cambiar la contraseña, se impide que el usuario reemplace inmediatamente la contraseña nueva por la contraseña anterior. Para obtener detalles, consulte la página del comando man `passwd`(1).

Asignación de roles

No es obligatorio que los usuarios tengan roles. Puede asignarse un solo usuario a más de un rol si esto concuerda con la política de seguridad del sitio.

Asignación de autorizaciones

Como en el SO Oracle Solaris, al asignar autorizaciones directamente a un usuario, se agregan autorizaciones nuevas a las existentes. En Trusted Extensions, primero se agregan las autorizaciones a un perfil de derechos y luego se asigna el perfil al usuario.

Asignación de perfiles de derechos

Como en el SO Oracle Solaris, el orden de los perfiles es importante. El mecanismo de los perfiles utiliza la primera instancia del comando o la acción del conjunto de perfiles de la cuenta.

Puede utilizar el orden de clasificación de perfiles para su beneficio. Si desea que un comando se ejecute con atributos de seguridad diferentes de los que se definen para el comando de un perfil existente, cree un perfil nuevo con las asignaciones preferidas para el comando. Luego, inserte ese perfil nuevo antes del perfil existente.

Cambio de valores predeterminados de privilegios

El conjunto de privilegios predeterminado puede ser demasiado liberal para varios sitios. A fin de restringir el conjunto de privilegios para cualquier usuario común en el sistema, cambie la configuración del archivo `policy.conf`. Para cambiar el conjunto de privilegios de los usuarios individuales, utilice Solaris Management Console. Si desea obtener un ejemplo, consulte Cómo restringir el conjunto de privilegios de un usuario.

Cambio de valores predeterminados de etiquetas

El cambio de los valores predeterminados de una etiqueta del usuario crea una excepción a los valores predeterminados del usuario en el archivo `label_encodings`.

Cambio de valores predeterminados de auditoría

Como en el SO Oracle Solaris, la asignación de clases de auditoría a un usuario crea excepciones a las clases de auditoría que se asignan en el archivo `/etc/security/audit_control` del sistema. Para obtener más información sobre auditoría, consulte el Capítulo 18Auditoría de Trusted Extensions (descripción general).

Mantenimiento

Marco de Referencia

ISO 22301: Sistema de Gestión basada en PDCA

ISO 31000: Gestión de Riesgos

La norma internacional ISO 22301, para gestión de continuidad de negocio, ha sido creada a partir de la demanda internacional que obtuvo la norma británica original BS-25999-2. Esta norma, identifica los fundamentos de un sistema de gestión de continuidad del negocio, estableciendo los procesos, principios y terminologías de gestión de continuidad de negocio.

Oracle Database Backup Cloud Service

Oracle Database Backup Cloud Service es una solución de Oracle para hacer respaldos de bases de datos Oracle en la nube pública y tiene 4 características:

- Segura: Protección de datos y políticas privadas.
- Confiable: Políticas de redundancia para asegurar que los datos son altamente disponibles.
- Escalable: Capacidad bajo demanda, esto es, se puede crecer rápidamente en capacidad de almacenamiento cuando se necesite.
- Simple: Gestión de respaldos transparente usando RMAN (Recovery Manager) para las operaciones de respaldo y recuperación por lo que no es necesario aprender nuevas herramientas o nuevos comandos.

Regla de respaldo 3 - 2 - 1

- Tener al menos 3 copias de sus datos.
- Almacenarlas en 2 medios diferentes.

- Tener 1 copia de respaldo en un medio externo.

BIBLIOGRAFÍA

https://docs.oracle.com/cd/E24842_01/html/E22519/manageusers-27.html
https://www.oracle.com/technetwork/es/database/enterprise-edition/documentation/seguridad-y-cumplimiento-normativo-2247283-esa.pdf
https://desktop.arcgis.com/es/arcmap/latest/extensions/data-reviewer-guide/admin-dr-oracle/transparent-data-encryption-tde-for-the-reviewer-workspace-in-oracle.htm#GUID-29749E61-D19B-45E2-84A9-CBC085650B5E
https://docs.oracle.com/cd/E11882_01/network.112/e40393/asotrans.htm#ASOAG9522
http://www.paolapullas.com/tech/2016/11/22/oracle-database-backup-cloud-service-conceptos/