Auditoria del S. G. B. D.

Auditoria de Seguridad:

- La auditoria crea un registro de las actividades seleccionadas que los usuarios realicen.

Objetivos:

- Detectar acciones inusuales o sospechosas
- Identificar a los usuarios específicos que han realizado estas acciones.
- Detectar intentos de acceso no autorizados
- Evaluar daños de seguridad potenciales

Auditoria del S. G. B. D.

Auditoria de Seguridad:

- Si existe separación de roles el usuario que puede ejecutar las herramientas de auditoria es el DBSSO (Data Base Security Office) y/o el AAO (Audit Analysis Officer)
- Si no existe separación de roles estas tareas las puede realizar el DBSA (Data Base System Administrator) generalmente el usuario “informix”

Auditoria herramienta onaudit

Herramienta onaudit

- onaudit
  - Configurar la auditoria del servidor y de las bases de datos creadas en él.
  - Permite administrar las máscaras para las auditorias y de las acciones realizadas por los distintos usuarios.

Herramienta onaudit

Mostrar Máscara de Auditoria

- onaudit –o
  - Muestra todas las máscaras definidas
- onaudit –o –u *nombre_máscara*
  - Muestra la información de la máscara indicada

Herramienta onaudit

Crear o agregar una Máscara de Auditoria

- onaudit –a …
    - Agregar una máscara de auditoria nueva
- onaudit –f *nombre_archivo*
    - Definir una o varias máscaras desde un archivo.

Herramienta onaudit

Agregar una nueva máscara

- onaudit –a –u fulano –e +INRW,UPRW,DLRW
  - Agregar una máscara de nombre “fulano” para el usuario “fulano”
  - Registra insert into (INRW), update (UPRW) y delete from (DLRW)

Herramienta onaudit

Modificar una máscara

- onaudit –m –u fulano –e –INRW –e +RDRW
  - Modifica la máscara de nombre “fulano” para el usuario “fulano”
  - Quita el registro de insert into (INRW)
  - Agrega el registro de leer fila (RDRW)

Herramienta onaudit

Eliminar una máscara

- onaudit –d –u fulano
- Elimina la máscara de nombre “fulano” para el usuario “fulano”

Herramienta onaudit

Inicio de un nuevo archivo de auditoria

- onaudit –n
- Crea un nuevo archivo para registrar las auditorias

Herramienta onaudit

Mostrar la configuración de auditoria

- onaudit –c
- Muestra la información del archivo de configuración
- El archivo se llama “adtcfg” y se encuentra dentro del directorio de instalación de informix en la carpeta “aaodir”

Herramienta onaudit

Archivo …/aaodir/adtcfg

- ADTMODE 1
  - Modo de la auditoria
- ADTPATH /opt/IBM/informix/auditar
  - Directorio donde se almacenan los archivos con las pistas de auditoria
- ADTSIZE 50000
  - Tamaño máximo de un archivo de auditoria

Herramienta onaudit

Iniciar la auditoria: onaudit –l *modo*

- Modos
  - 1: activa la auditoría para todas las sesiones, pero no audita automáticamente las acciones del DBSSO ni del DBSA.
  - 3: activa la auditoría y audita automáticamente las acciones del DBSSO.
  - 5: activa la auditoría y audita automáticamente las acciones del DBSA.
  - 7: activa la auditoría y audita automáticamente todas las acciones del DBSSO y del DBSA, incluyendo los sucesos _exclude.

Auditoria herramienta onshowaudit

Herramienta onshowaudit

- onshowaudit
  - Permite extraer la información registrada en las distintas pistas de auditoria.
  - Se puede especificar un usuario o un servidor determinado

Herramienta onshowaudit

- onshowaudit
  - Esta herramienta solo puede ser ejecutada por el usuario:
    - A.A.O. (con separación de roles)
    - informix (sin separación de roles)

Herramienta onshowaudit

- onshowaudit
  - Al ejecutar la herramienta sin parámetros se extrae toda la información de la auditoria.
  - Para todos los usuarios y para todos los servidores

Herramienta onshowaudit

- onshowaudit –u *nombre_usuario*
  - Solo se muestra las pistas correspondientes al usuario indicado

Herramienta onshowaudit

- onshowaudit –f *nombre_archivo* –u *nombre_usuario*
  - Solo se muestra las pistas correspondientes al usuario indicado en el archivo indicado