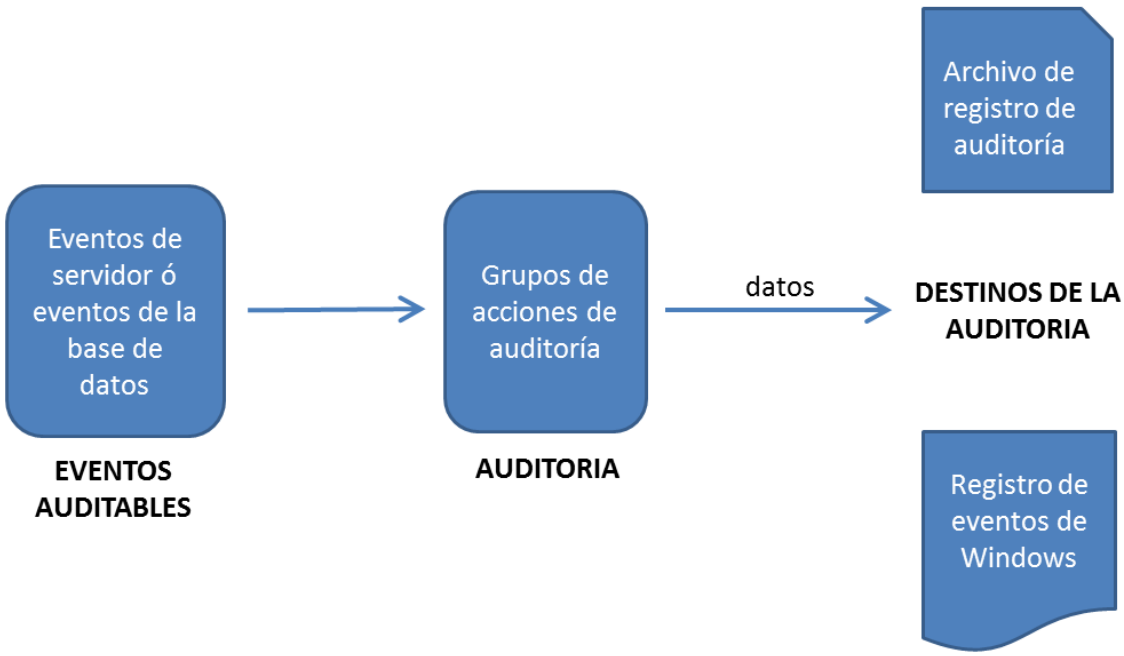
Auditoría en SQL SQLSERVER (SQL Server Audit)



Se entiende por auditoría al proceso de seguimiento y registro de los eventos que se producen en el Motor de base de datos (database engine). La auditoría puede ser:

- **A nivel de servidor:** contiene especificaciones de auditoría para los eventos del servidor.
- **A nivel de base de datos:** contiene especificaciones de auditoría para los eventos de base de datos.

Los datos de los eventos auditados se escriben en los archivos de registro de auditoría ó en el registro de eventos de Windows.

Procedimiento para crear una auditoría

1. Crear la auditoría y definir el destino de los datos de los eventos auditados.
2. Crear una especificación de auditoría y habilitarla. Una especificación de auditoría puede incluir varios grupos de acciones de auditoría ó acciones de auditoría.
3. Habilitar la auditoría.
4. Leer el destino de la auditoría.

Grupos de acciones de auditoría

A continuación se muestra algunos grupos de acciones de auditoría.

A nivel de servidor

- AUDIT_CHANGE_GROUP: el evento se desencadena cuando se crea, modifica ó elimina una especificación de auditoría.
- BACKUP_RESTORE_GROUP: el evento ocurre cuando se emite un comando de copia de seguridad ó de restauración.
- DATABASE_CHANGE_GROUP: el evento se desencadena cuando se crea, modifica ó elimina una base de datos.
- DATABASE_OBJECT_CHANGE_GROUP: el evento ocurre cuando se crea, modifica ó elimina un objeto de la base de datos.
- FAILED_LOGIN_GROUP: el evento ocurre cuando una entidad de seguridad intenta iniciar una sesión SQL Server y no lo consigue.

A nivel de base de datos

Muchos de los grupos de acciones de auditoría a nivel de servidor se pueden especificar también a nivel de base de datos.

- DBCC_GROUP: el evento ocurre cuando una entidad de seguridad emite un comando DBCC.
- SCHEMA_OBJECT_CHANGE_GROUP: el evento se desencadena al realizar una operación CREATE, ALTER o DROP en un esquema.
- SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP: el evento se desencadena cuando se emite una concesión, denegación o revocación en un objeto de esquema.
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP: el evento ocurre cuando una entidad de seguridad inicia una sesión en una base de datos.
- USER_CHANGE_PASSWORD_GROUP: el evento ocurre cuando se cambia la contraseña de un usuario de base de datos utilizando la instrucción ALTER USER.

A nivel de auditoría

Audita las acciones del propio proceso de auditoría.

AUDIT_ CHANGE_GROUP: el evento se desencadena al emitir uno de los comandos siguientes:

- CREATE SERVER AUDIT
- ALTER SERVER AUDIT
- DROP SERVER AUDIT
- CREATE SERVER AUDIT SPECIFICATION
- ALTER SERVER AUDIT SPECIFICATION
- DROP SERVER AUDIT SPECIFICATION
- CREATE DATABASE AUDIT SPECIFICATION
- ALTER DATABASE AUDIT SPECIFICATION
- DROP DATABASE AUDIT SPECIFICATION

Ejercicio: Auditoria de servidor

Crear la auditoría de servidor

1. SQL Server Management Studio, Explorador de objetos, Seguridad.
2. Clic secundario en Auditorías, Nueva auditoría.
3. Página General: defina las propiedades generales de la auditoría. El destino será un archivo de registro de auditoría. Clic en Aceptar.

Crear una especificación de auditoría de servidor

1. SQL Server Management Studio, Explorador de objetos, Seguridad.
2. Clic secundario en Especificaciones de auditoría de servidor, Nueva especificación de auditoría de servidor.
3. En Auditoría: seleccione la auditoría a la que pertenece la especificación.
4. En Tipo de acción de auditoría: seleccione un grupo de acciones de auditoría. Por ejemplo: DATABASE_OBJECT_CHANGE_GROUP y FAILED_LOGIN_GROUP. Clic en Aceptar.

Habilitar la especificación de auditoría de servidor

1. En Seguridad, expanda Especificaciones de auditoría de servidor.
2. Clic secundario en la especificación de auditoría de servidor, Habilitar especificación de auditoría de servidor.

Habilitar la auditoría de servidor

1. En Seguridad, expanda Auditorías.
2. Clic secundario en la auditoría de servidor, Habilitar auditoría.

Probando la auditoría de servidor

1. Abra una ventana de consulta y en la base de datos Northwind cree una tabla T1 con una columna numérica entera.
2. Intente iniciar una nueva conexión con un login SQL inexistente.

Leer el archivo de registro de auditoría

1. En Seguridad, expanda Auditorías.
2. Clic secundario en la auditoría de servidor, Ver registros de auditoría.

Ejercicio: Auditoria de base de datos

Crear la auditoría de servidor

1. SQL Server Management Studio, Explorador de objetos, Seguridad.
2. Clic secundario en Auditorías, Nueva auditoría.
3. Página General: defina las propiedades generales de la auditoría. El destino será un archivo de registro de auditoría. Clic en Aceptar.

Crear una especificación de auditoría de base de datos

1. SQL Server Management Studio, Explorador de objetos, Bases de datos, expanda Northwind.
2. Expanda Seguridad, clic secundario en Especificaciones de auditoría de base de datos, Nueva especificación de auditoría de base de datos.
3. En Auditoría: seleccione la auditoría a la que pertenece la especificación.
4. En Tipo de acción de auditoría: seleccione un grupo de acciones de auditoría. Por ejemplo: DATABASE_OBJECT_CHANGE_GROUP.
5. En Tipo de acción de auditoría: seleccione DELETE.
6. En Clase de objeto: seleccione OBJECT.
7. En Nombre de objeto: seleccione [Order details].
8. En Nombre de la entidad de seguridad: seleccione dbo.
9. Clic en Aceptar.

Habilitar la especificación de auditoría de servidor

1. En Seguridad, expanda Especificaciones de auditoría de base de datos.
2. Clic secundario en la especificación de auditoría de base de datos, Habilitar especificación de auditoría de base de datos.

Habilitar la auditoría de servidor

1. En Seguridad, expanda Auditorías.
2. Clic secundario en la auditoría de servidor, Habilitar auditoría.

Probando la auditoría de servidor

1. Abra una ventana de consulta y en la base de datos Northwind cree una tabla T2 con una columna numérica entera.
2. Ejecute el comando para eliminar filas de la tabla [Order details].

Leer el archivo de registro de auditoría

1. En Seguridad, expanda Auditorías.
2. Clic secundario en la auditoría de servidor, Ver registros de auditoría.

Nota: también puede leer los archivos de registro de auditoría con la función **sys.fn_get_audit_file**.

Ejercicio: uso de desencadenantes DDL para seguimiento de cambios en los datos

A ser resuelto en el aula.