GUÍA DE AUDITORIAS DE SQL SERVER

César Ovidio Martínez Chicas

Monitoreo general de eventos ocurridos en el SGBD SMSS

SQL Server Audit proporciona a los DBA la capacidad de capturar auditorías granulares contra la actividad a nivel de instancia y base de datos y guardar esta actividad en un archivo. La ubicación donde se guardan los datos de auditoría se conoce como destino. El objeto de auditoría de SQL Server se encuentra en el nivel de instancia y define las propiedades de la auditoría y el objetivo. Puede tener múltiples auditorías de servidor en cada instancia. Esto es útil si tiene que auditar muchos eventos en un entorno ocupado, ya que puede distribuir el IO utilizando un archivo como destino y colocando cada archivo de destino en un volumen separado.

Al crear una auditoría, puede usar las opciones detalladas en la siguiente tabla:

Opción	Descripción
FILEPATH	Con esta opción se debe seleccionar donde se quiere guardar el resultado de la auditoría
MAXSIZE	Esta opción especifica el tamaño máximo que puede tener el archivo resultante de la auditoría
MAX_ROLLOVER_FILES	Solo se aplica si elige un destino de archivo. Cuando el archivo de auditoría se llena, puede hacer un ciclo de ese archivo o generar un archivo nuevo.
MAX_FILES	Limita la cantidad máxima de archivos que pueden ser generados durante la auditoría
QUEUE_DELAY	Especifica si los eventos de auditoría son escritos de manera sincrónica o asíncrona.
ON_FAILURE	Especifica que debe suceder en caso de un fallo. Las opciones disponibles son: CONTINUE, SHUTDOWN y FAIL_OPERATION

Puede crear una auditoría de servidor a través de la GUI en SQL Server Management Studio al profundizar en Seguridad en el Explorador de objetos y elegir Nueva auditoría en el nodo Auditorías.

Antes de comenzar esta práctica, es importante saber que para replicarla se deben tener ciertos elementos preconfigurados:

- Base de datos restoreDB
- Login sencillo “Auditor1”

Parte I - Creando una nueva auditoría

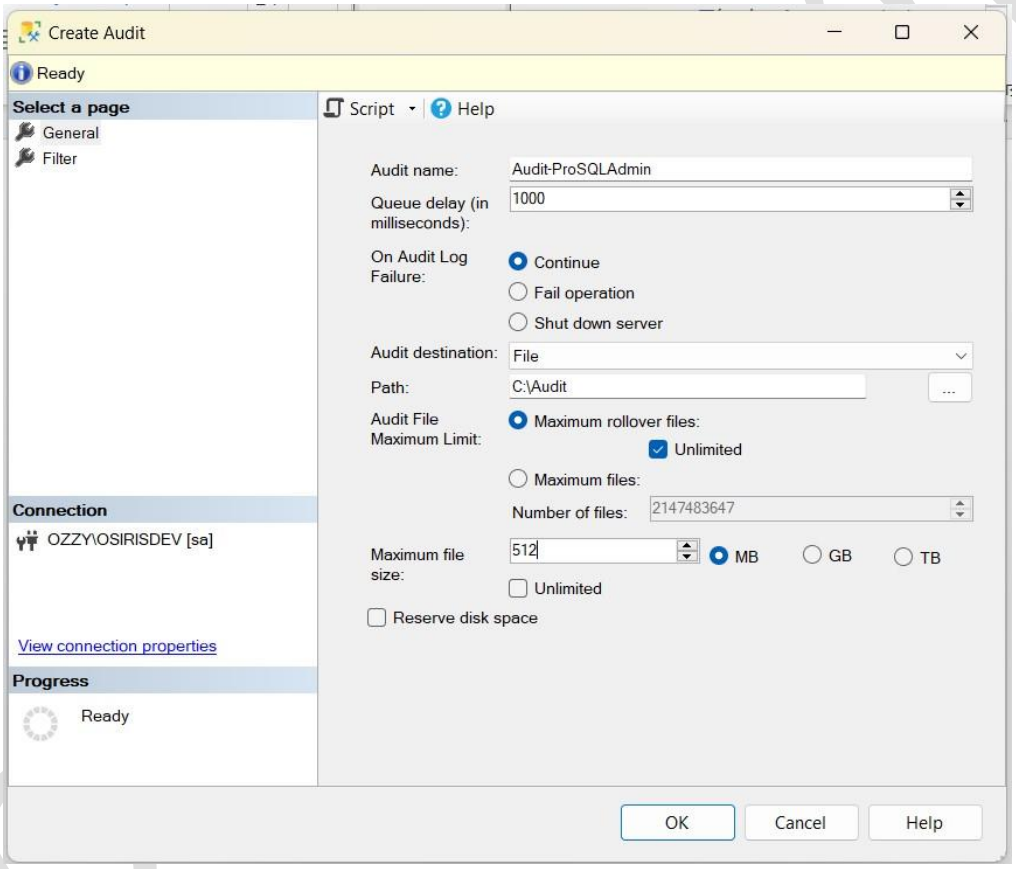
Paso 1:

En el explorador de objetos de SQL Server, despliegue la opción de “Seguridad” y luego haga clic derecho sobre “New Audit”.

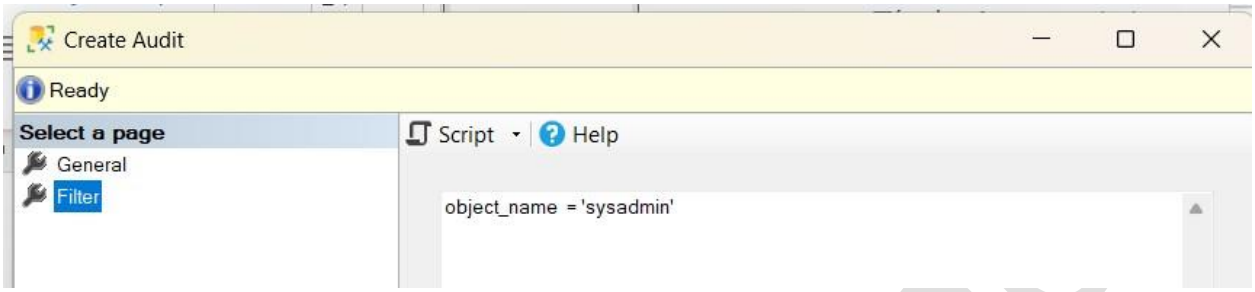
Paso 2:

En la pantalla de “Create Audit”, establecer los valores mostrados.

Esta configuración guardará nuestra auditoría en un archivo plano, en lugar de un registro de Windows. Por lo tanto, necesitamos especificar los parámetros relacionados con el archivo. Configuramos nuestro archivo para que se transfiera y aplicamos el tamaño máximo para el archivo de 512 MB. Dejamos el valor predeterminado de 1 segundo (1000 milisegundos) como una duración máxima antes de que las entradas de auditoría se escriban en el registro y nombren la auditoría Audit-ProSQLAdmin.



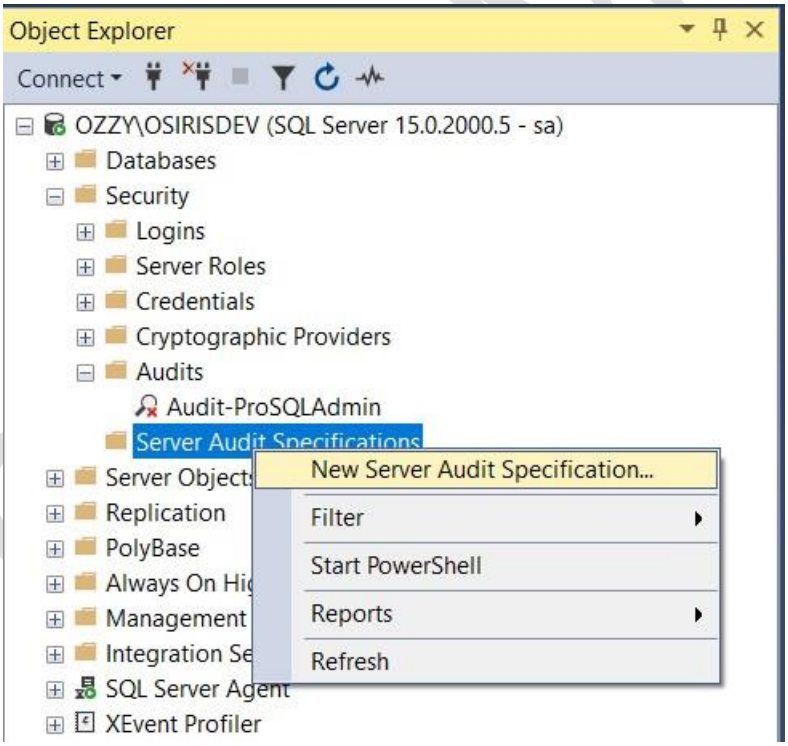
En la pestaña Filtro del cuadro de diálogo Crear auditoría, especificamos que deseamos filtrar por nombre_objeto y solo auditar los cambios en la función de administrador del sistema (sysadmin)



Parte II - Creando una especificación de auditoría

Paso 1

Ubicamos la carpeta “Server Audit Specifications”, hacemos clic derecho y seleccionamos “New Server Audit Specification…”

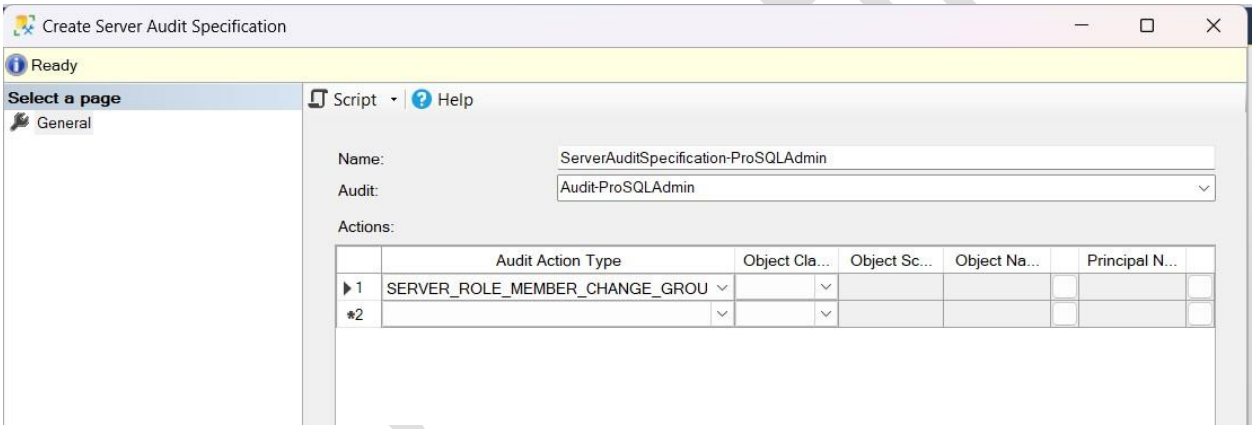


Paso 2

Establecer los valores indicados en la pantalla.

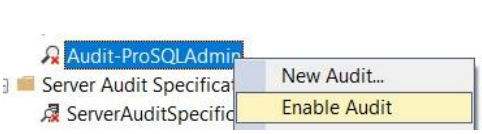
Hemos seleccionado SERVER_ROLE_MEMBER_CHANGE_GROUP como el tipo de acción de auditoría.

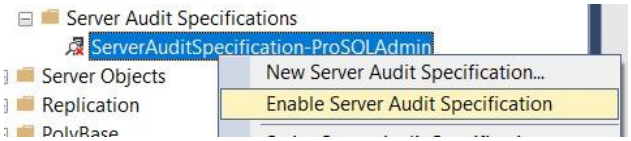
Esto audita las adiciones o eliminaciones de la membresía de los roles de servidor. Sin embargo, combinado con el filtro que hemos puesto en el objeto Auditoría del servidor, el nuevo resultado es que solo se registrarán los cambios en la función del servidor sysadmin. También seleccionamos la auditoría Audit-ProSQLAdmin del cuadro desplegable Audit para unir los objetos.



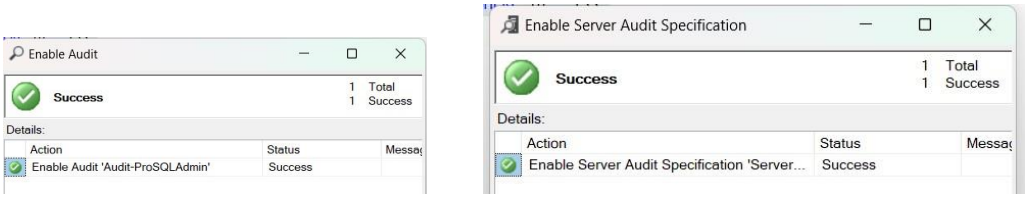
Paso 3

Aunque hemos creado la auditoría del servidor y la especificación de auditoría del servidor, debemos habilitarlas antes de que se comience a recopilar cualquier dato. Podemos lograr esto seleccionando Habilitar en el menú contextual de cada uno de los objetos en el Explorador de objetos, o modificando los objetos y configurando su ESTADO = ENCENDIDO en T-SQL.





Esto mostrará los mensajes:



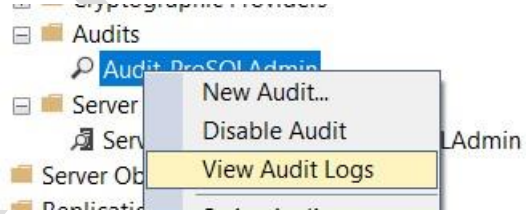
Paso 4

Ahora que están habilitados los elementos de auditoría, debemos alterar el Login “Auditor1”, al cual agregaremos a los roles de “serveradmin” y “sysadmin”. Puede hacerse gráficamente o a través del siguiente comando:

```
ALTER SERVER ROLE serveradmin ADD MEMBER Auditor1 ;
ALTER SERVER ROLE sysadmin ADD MEMBER Auditor1 ;
```

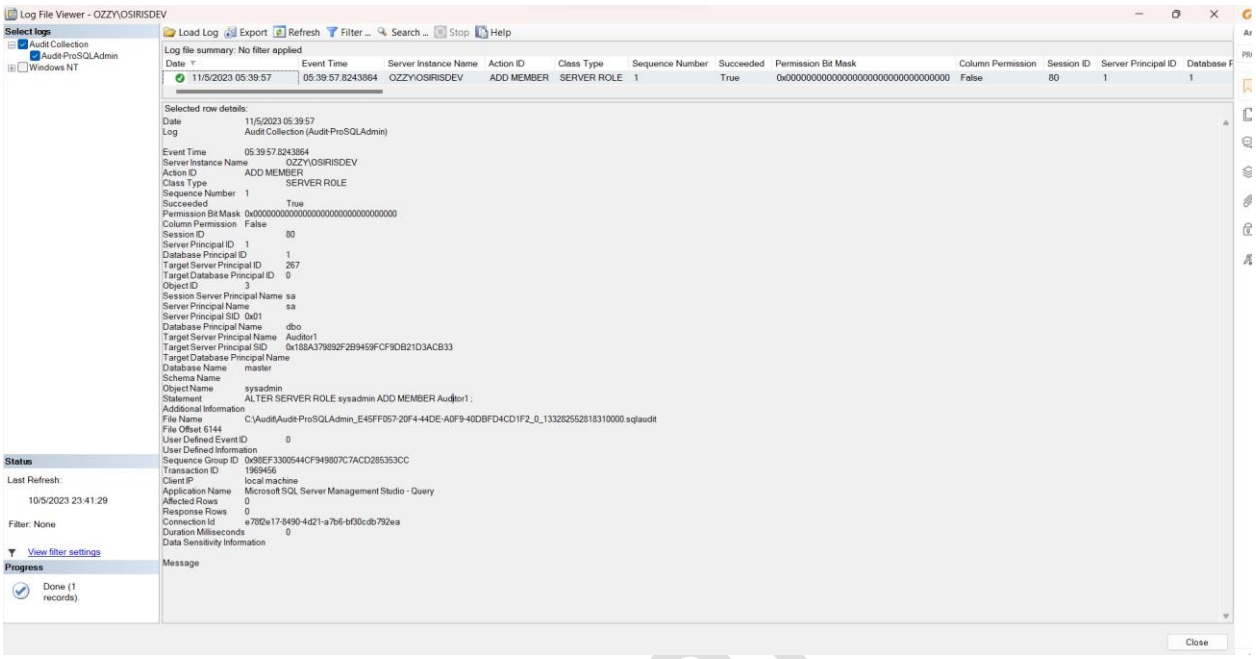
Paso 5

Es momento de verificar si se están registrando los eventos especificados, para ello hacemos clic derecho sobre la Auditoría creada “Audit ProSQLAdmin” y seleccionamos la opción “View Audit Logs”



Al hacerlo se mostrará la siguiente ventana conteniendo los registros de auditoría.

Podemos ver que se ha capturado un nivel granular de información. En particular, esta información incluye la declaración completa que provocó que se activara la auditoría, la base de datos y el objeto involucrados, el inicio de sesión de destino y el inicio de sesión que ejecutó la declaración.



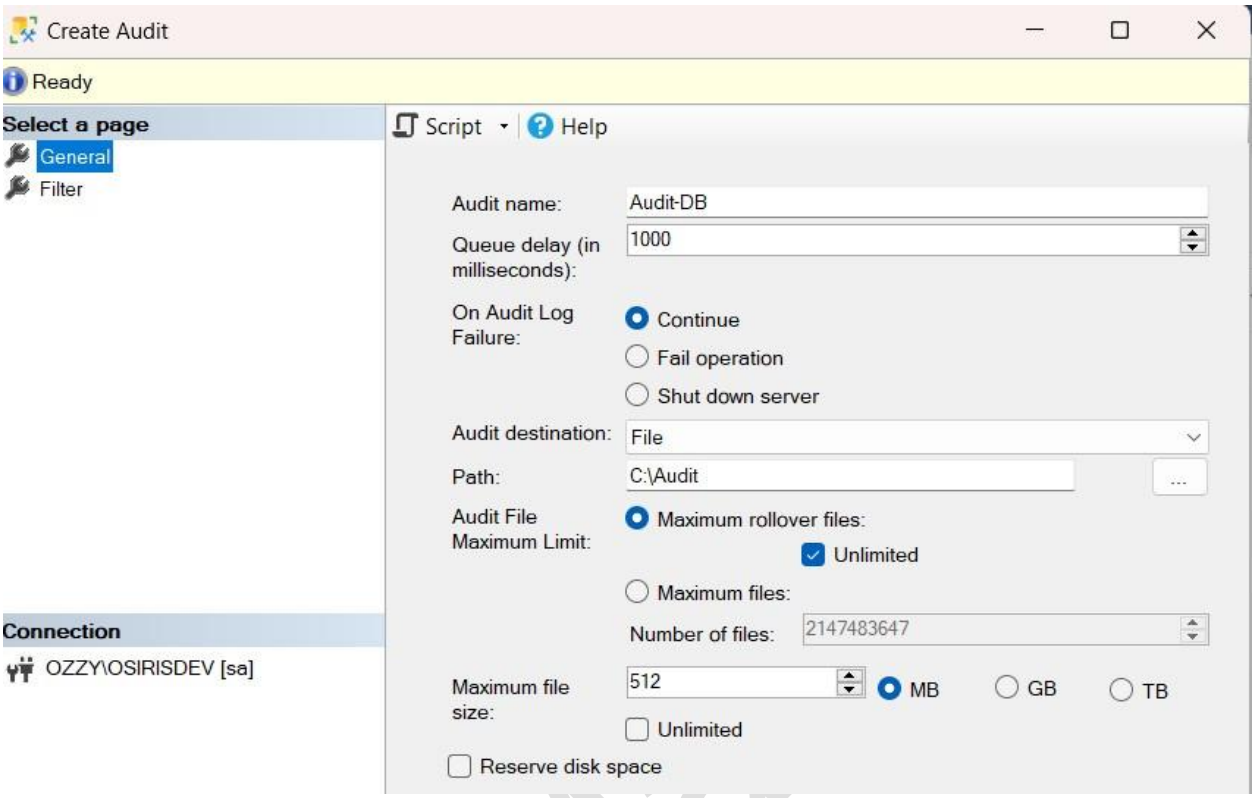
Parte III - DATABASE AUDIT SPECIFICATIONS

Una especificación de auditoría de base de datos es similar a una especificación de auditoría de servidor, pero especifica requisitos de auditoría a nivel de base de datos, en lugar de a nivel de instancia.

Para demostrar esta funcionalidad, asignamos el inicio de sesión de “Auditor1” a un usuario en esta base de datos y asignamos permisos SELECT a la tabla Empleado. También creamos una nueva auditoría de servidor, llamada ServerAuditDB, que usamos como la auditoría a la que se adjunta nuestra especificación de auditoría de base de datos.

Paso 1

Crear la nueva auditoría según la imagen siguiente:



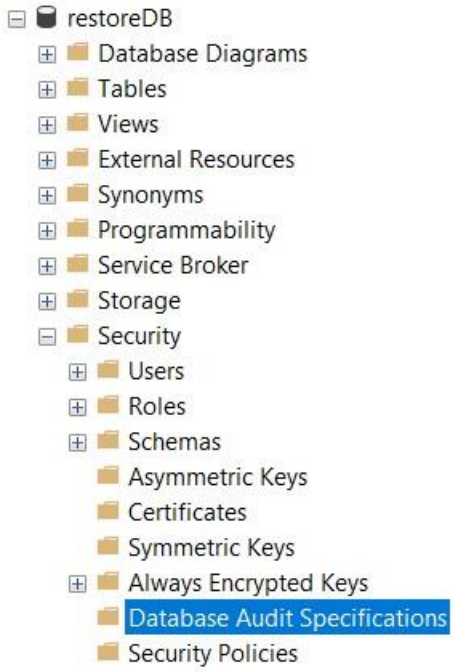
Paso 2

Ubicarse en la base de datos “restoreDB”, mapear el Login Auditor1 a un usuario dentro de la base de datos y otorgarle permisos de selección.

```
use restoreDB;

CREATE USER Auditor1 FOR LOGIN Auditor1 WITH DEFAULT_SCHEMA=dbo;
GRANT SELECT ON dbo.Empleado TO Auditor1;
```

Paso 3

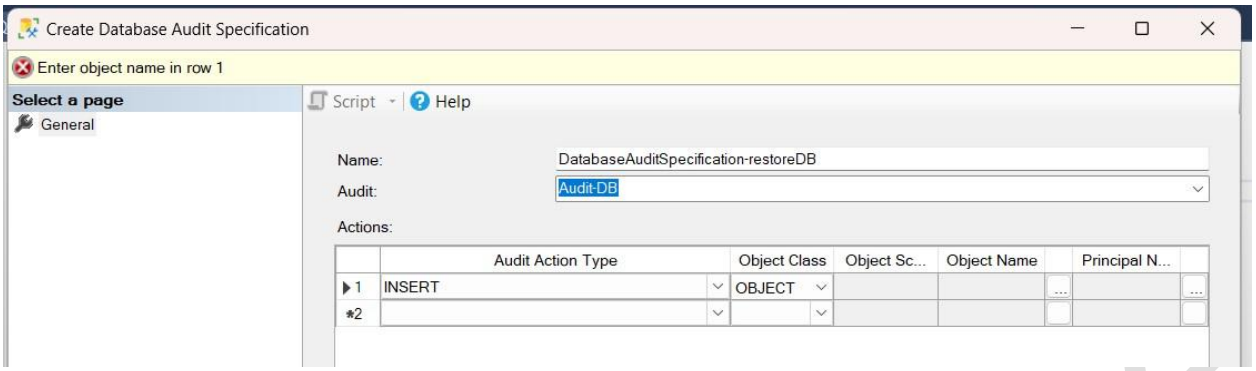
Crear la especificación de auditoría de base de datos, para ello desplegamos la carpeta “Security” de la base “restoreDB”, y hacemos clic derecho sobre “Database Audit Specification”

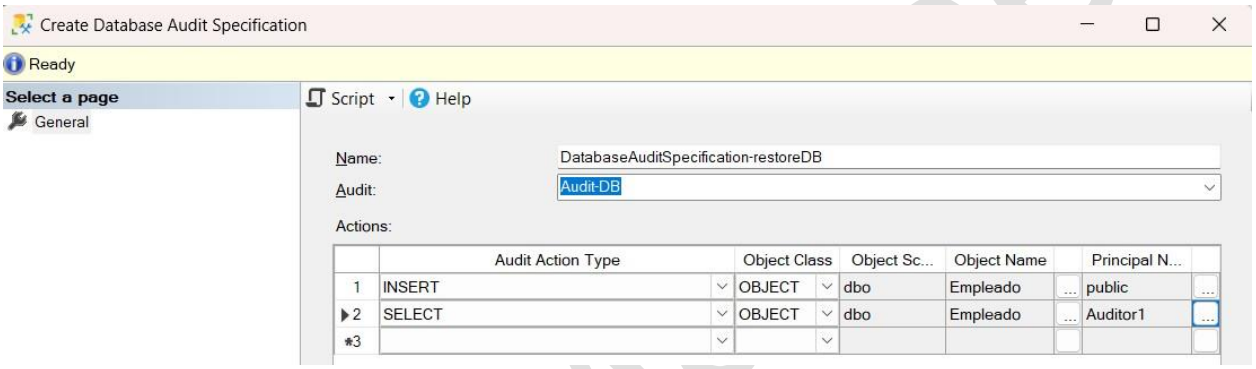


Paso 4

Establecer los elementos que se auditarán.

Ahora buscamos crear una especificación de auditoría de base de datos que capture cualquier declaración INSERT hecha contra la tabla Empleado por cualquier usuario, pero también captura declaraciones SELECT ejecutadas específicamente por Auditor1.





En la mitad inferior de la pantalla, especificamos dos tipos de acciones de auditoría, INSERT y SELECT. Debido a que especificamos una clase de objeto de OBJECT, a diferencia de las otras opciones disponibles de DATABASE o SCHEMA, también debemos especificar el nombre de objeto de la tabla que queremos auditar. Como solo queremos que se audite la actividad SELECT del Auditor1, agregamos este usuario al campo Principal para el tipo de acción SELECT, pero agregamos el rol Público como el principal para el tipo de acción INSERT. Esto se debe a que todos los usuarios de la base de datos serán miembros del rol Público y, por lo tanto, se capturará toda la actividad INSERT, independientemente del usuario.

Paso 5

Es momento de habilitar los elementos de auditoría, haciendo uso de los comandos:

```
ALTER DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification-restoreDB]
WITH (STATE = ON) ;

USE Master

ALTER SERVER AUDIT [Audit-DB] WITH (STATE = ON) ;
```

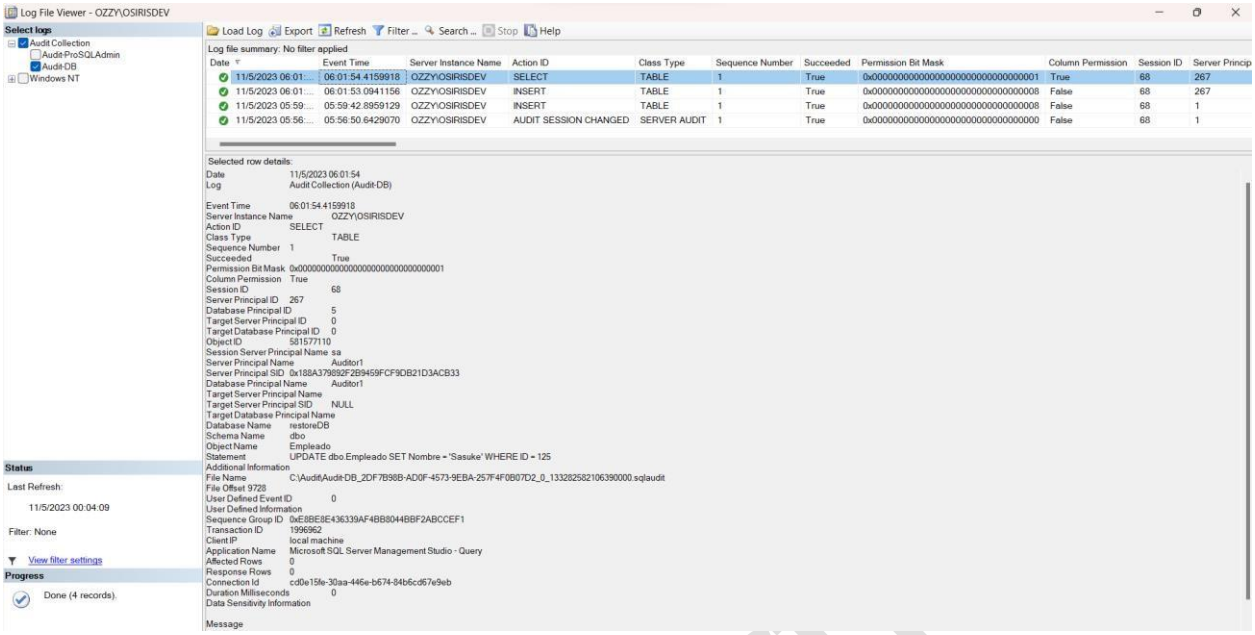
Puede notar que, para el primer query aún no encontramos sobre la base “restoreDB”, allí habilitamos la especificación de auditoría, luego nos colocamos sobre “master” y desde allí habilitamos la Auditoría.

Paso 6

Debido al paso 5 aún estamos en la base “master”, nos colocamos de nuevo sobre “restoreDB” y realizamos las pruebas:

```
--Pruebas
use restoreDB;
GRANT INSERT, UPDATE ON dbo.Empleado TO Auditor1;

INSERT INTO dbo.Empleado(id, Nombre, Apellido, Telefono) VALUES (15, 'Juan', 'Perez', 123456789) ;

UPDATE dbo.Empleado SET Nombre = 'Miguel' WHERE ID = 15 ;

EXECUTE AS USER ='Auditor1'

INSERT dbo.Empleado(id, Nombre, Apellido, Telefono) VALUES (125, 'Naruto', 'Uchiha', 123456789) ;

UPDATE dbo.Empleado SET Nombre = 'Sasuke' WHERE ID = 125 ;

REVERT
```

Hecho esto, verificamos los registros de auditoría y nos encontraremos con información similar a la que se muestra en la imagen siguiente:



Y con esto se concluye la configuración de una auditoría básica.