Webinar Gratis

Auditorías nativas de seguridad en SQL Server

Maximiliano Accotto

Acerca de mi

- Argentino nacido el 8 de agosto de 1977
- Data platform Geek
- Microsoft MVP Data Platform desde el 2005 a 2019.
- Speaker internacional en donde impartí mas de 500 charlas en los últimos 15 años.
- Especialista en tecnologías de Data y BI con mas de 20 años de trayectoria.
- Miembro de SQLPass, Microsoft User Group.

Maximiliano Accotto
Owner **Triggerdb SRL**

@maxiaccotto
https://ar.linkedin.com/in/maxiaccotto
https://blogs.triggerdb.com

Sobre TriggerDB

TriggerDB Consulting SRL es una empresa Argentina fundada por **Maximiliano Accotto** ,
experto reconocido a nivel mundial en Microsoft SQL Server y BI.

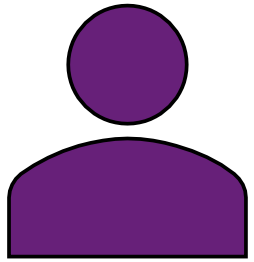
Somos partner certificados de Microsoft en las competencias de SQL Server, Data Analytics y Powerbi.

Contamos con mas de 15 años de trayectoria , alto expertice y cientos de clientes en América y Europa.

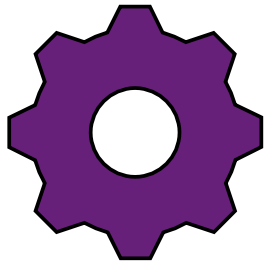
Microsoft Silver Partner

POWER BI PARTNER

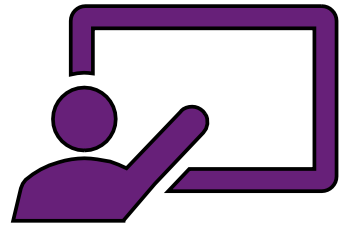
Servicios que ofrecemos



Consultoría



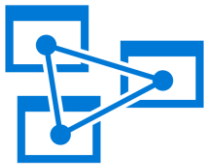
Soporte Premier



Entrenamiento

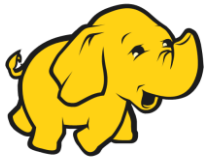
Productos en los que trabajamos

SQL Server



Analysis Services

Azure Data Factory



HDInsight

PowerBI

Azure
SQL Data Warehouse

Azure
Data Lake

Machine
Learning

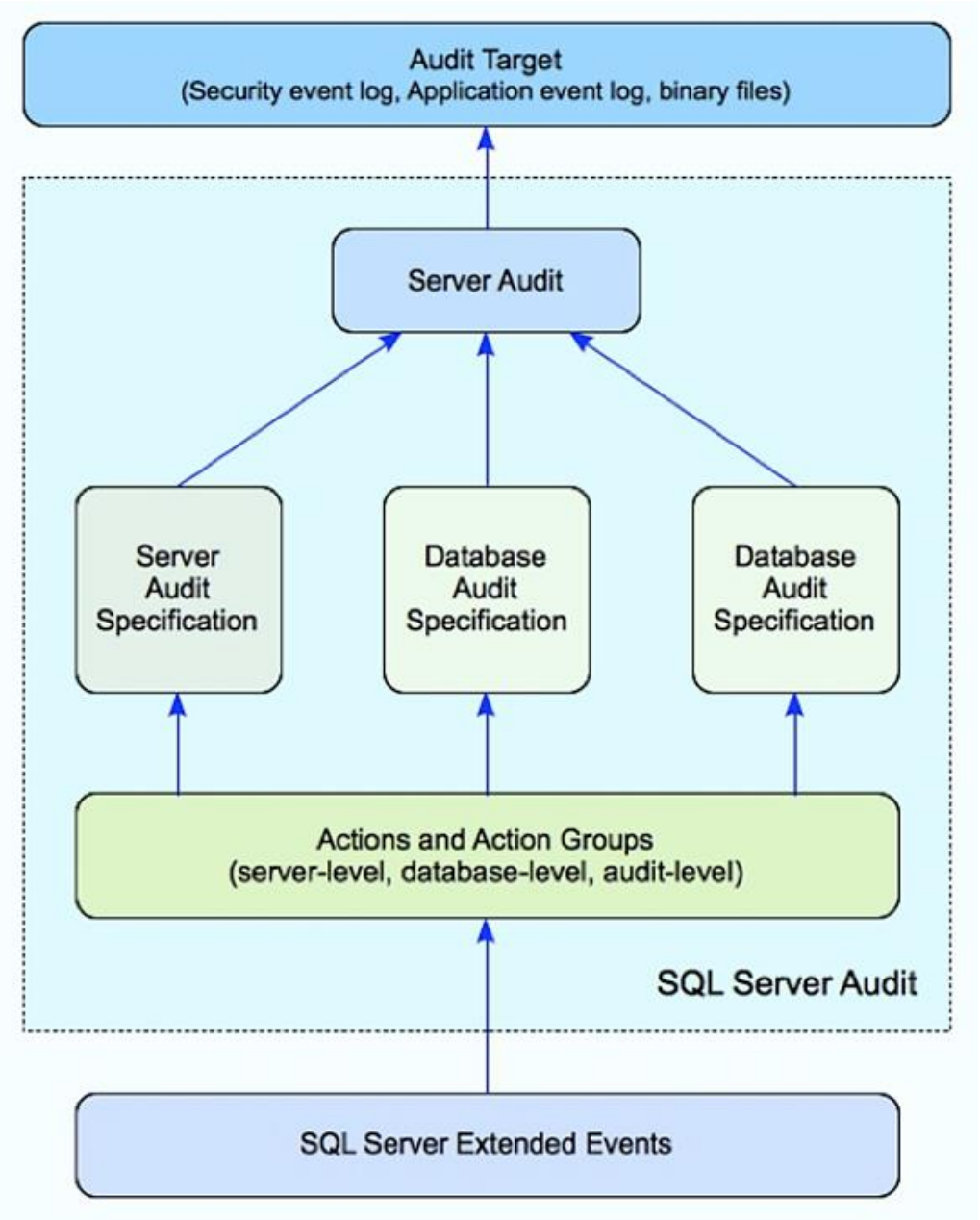
Azure SQL Server

Power Pivot
Power Query

Introducción

- Existen en MSSQL desde su versión 2008
  - En 2008 solo estaba disponible para Enterprise Edition
  - EN SQL 2012 se libero parte para Standard Edition
  - A partir de SQL 2016 esta disponible 100% en Standard Edition ☺
- No genera sobrecarga en el servidor
- Trabaja de forma asincrónica
- Utiliza Extended events
- No es data tracking
- Se pueden auditar eventos a nivel instancia o base de datos
- Se pueden guardar en archivos encriptados , security o application log
- Solo están soportadas para **SQL Server** o Azure **SQL Managed Instance.**
- En SQL 2019 se agrego la opción de datos sensibles

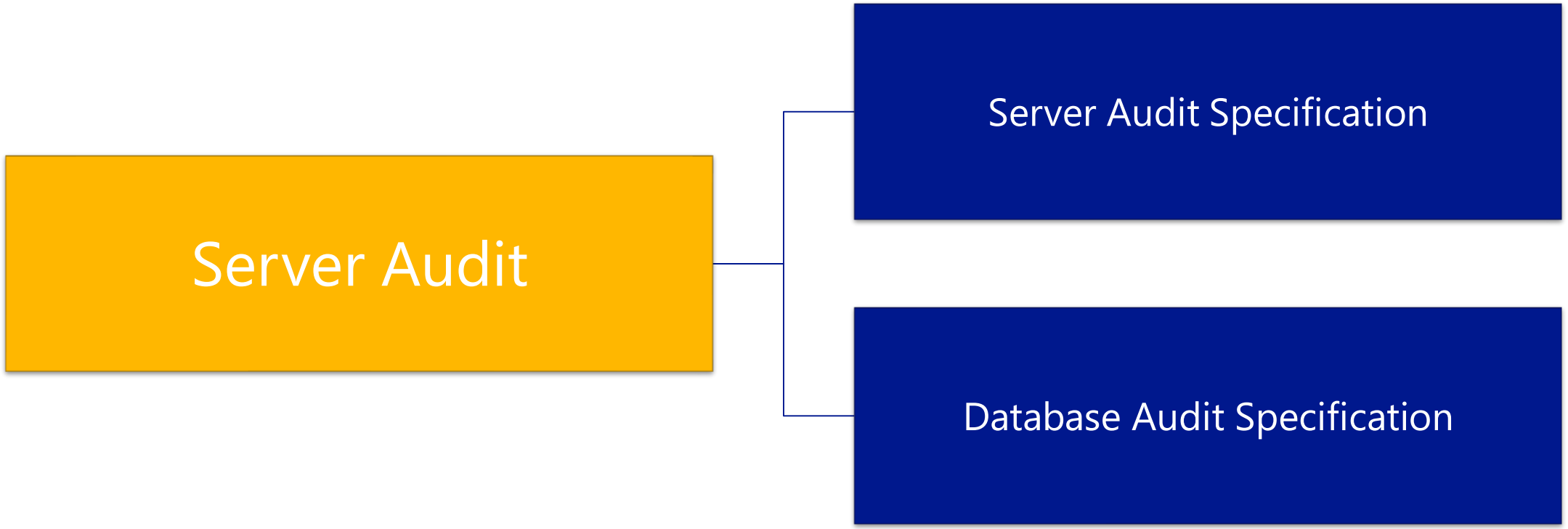
Arquitectura



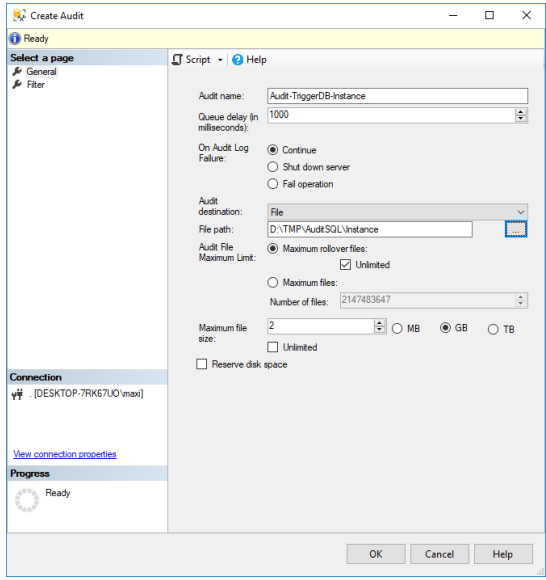
Componentes

Server Audit	Es el objeto principal, aquí se definen por ejemplo los lugares de persistencia de las auditorias (file, security Log o Application Log). Se pueden crear más de uno a nivel instancia
Server Audit Specifications	Permite auditar eventos a nivel instancia por ej. (Login Fail, créate database, etc.)
Database Audit Specifications	Permite auditar eventos a nivel base de datos por ej. (Select, insert, alter, etc) Es necesario que exista un Server Audit y se crean a nivel base de datos, por cada una de las que se desea tener este tipo de auditoria

Componentes II



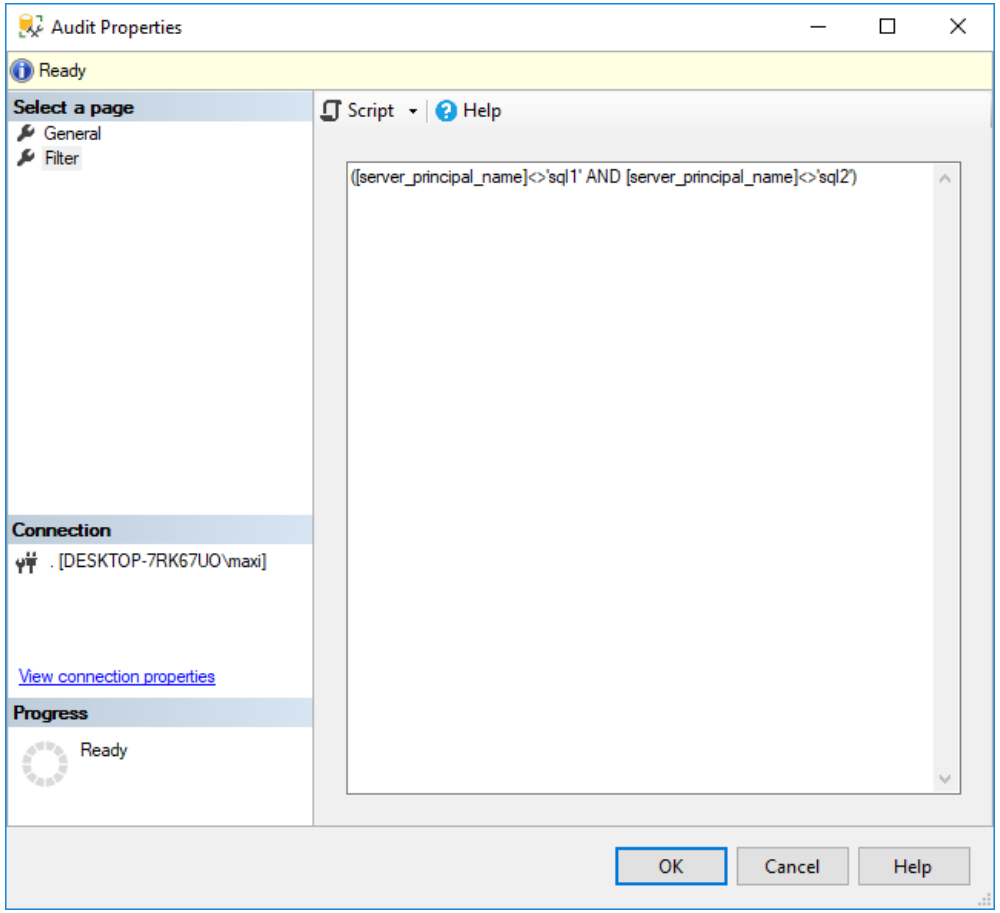
Server Audit



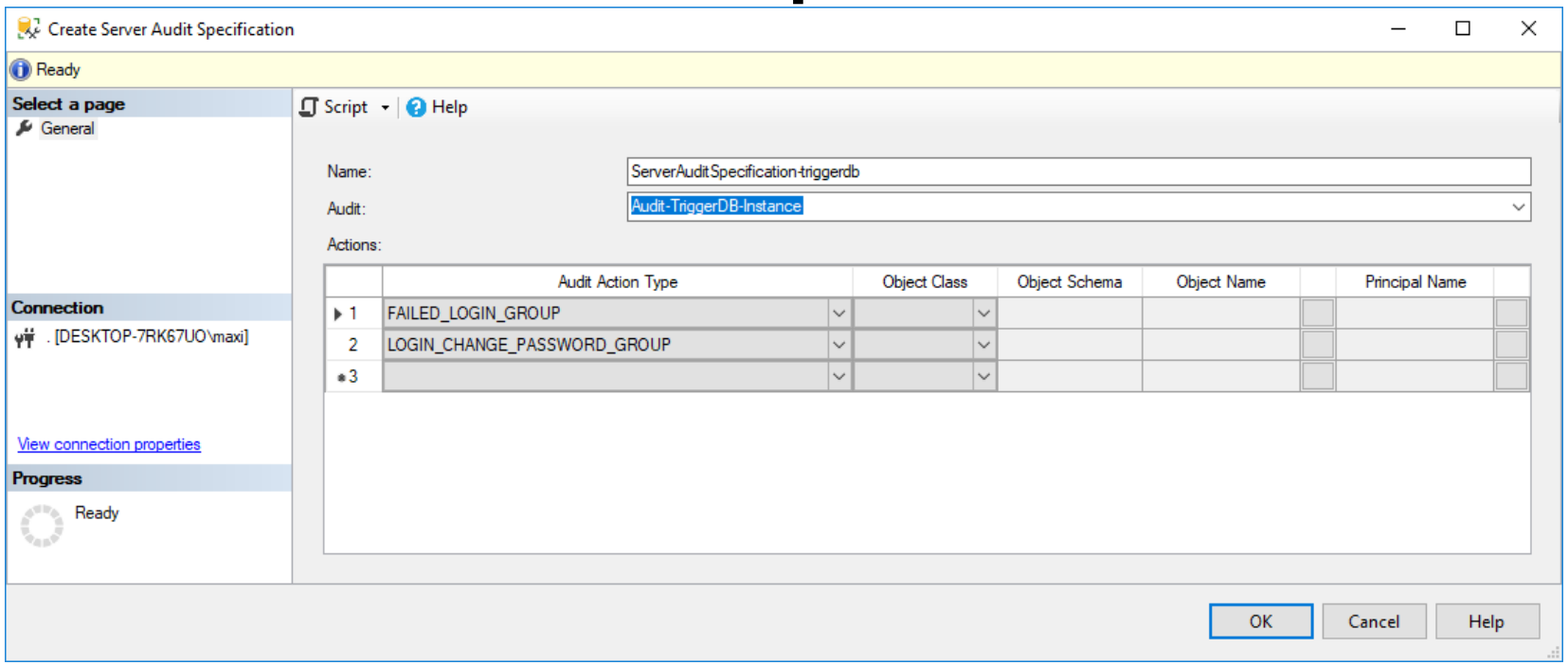
Audit Name	**Aquí debemos escribir el nombre del Server Audit.**
Queue delay	Especifica la cantidad de tiempo, en milisegundos, que puede transcurrir antes de exigir que se procesen las acciones de auditoría. El valor 0 indica la entrega sincrónica. El valor mínimo predeterminado es 1000 (1 segundo).
On Audit Log Failure	**Continue**: Las operaciones de continúan. Los registros de auditoría no se conservan. La auditoría continúa intentando el registro de eventos y se reanudará si se resuelve la condición de error. La selección de la opción Continuar puede permitir que una actividad no se audite. Esta es la selección predeterminada **Shut Down Server**: Fuerza el apagado del servidor cuando la instancia de servidor que escribe en el destino no puede escribir datos. Seleccione esta opción si un error de auditoría puede poner en peligro la seguridad o la integridad del sistema. **Fail Operation:** En los casos en que SQL Server Audit no puede escribir en el registro de auditoría, esta opción haría que las acciones de base de datos produjesen un error si generasen eventos auditados. Las acciones que no producen eventos auditados pueden continuar. La auditoría continúa intentando el registro de eventos y se reanudará si se resuelve la condición de error. Seleccione esta opción si el mantenimiento de una auditoría completa es más importante que el acceso total al Motor de base de datos.
Audit Destination	File , security Log o Application Log
File path	La ruta donde se guardarán los archivos.
Maximum file Size	Por defecto esta opción deja tener tamaño ilimitado

Server Audit Filter

- Los filtros evitan capturar eventos innecesarios
- Por ejemplo se podría excluir a los logins de aplicaciones.
- Se utilizan los campos del dataset resultante de la auditoria https://docs.microsoft.com/en-us/sql/relational-databases/system-functions/sys-fn-get-audit-file-transact-sql?view=sql-server-ver15

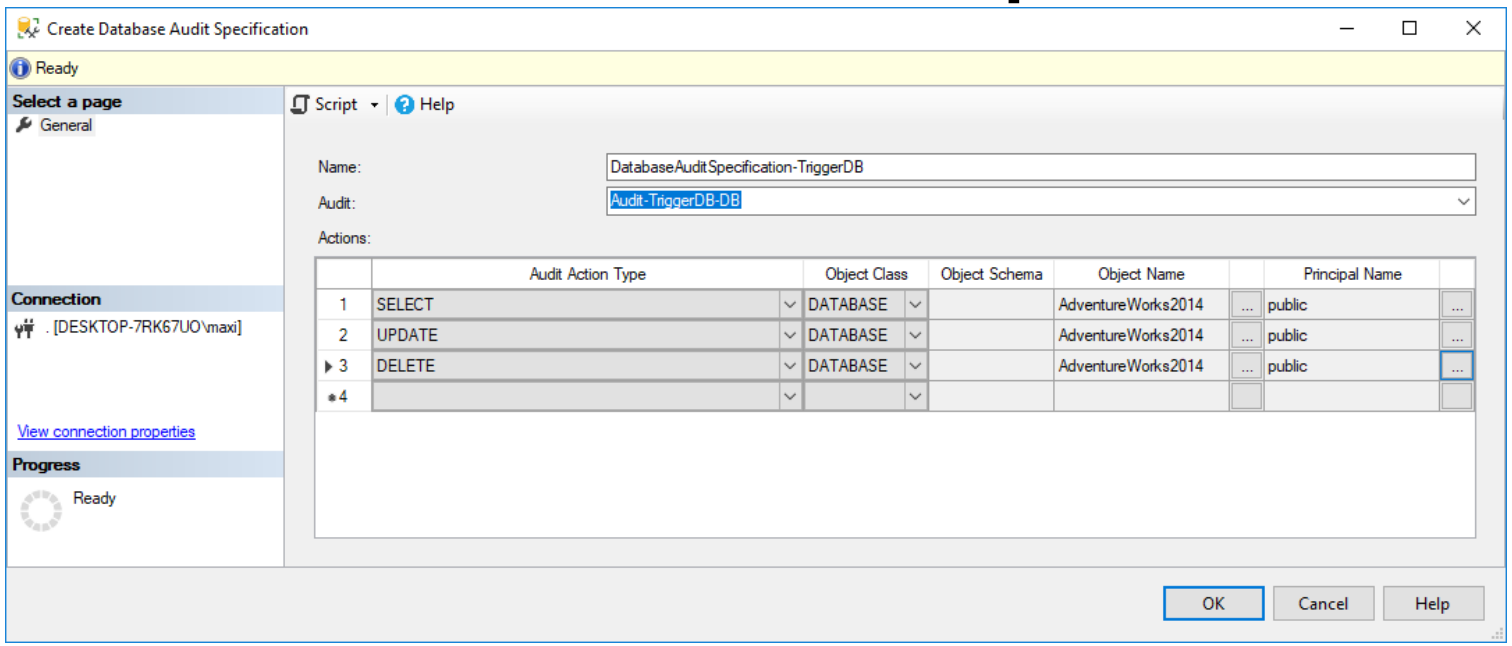


Server Audit Specification



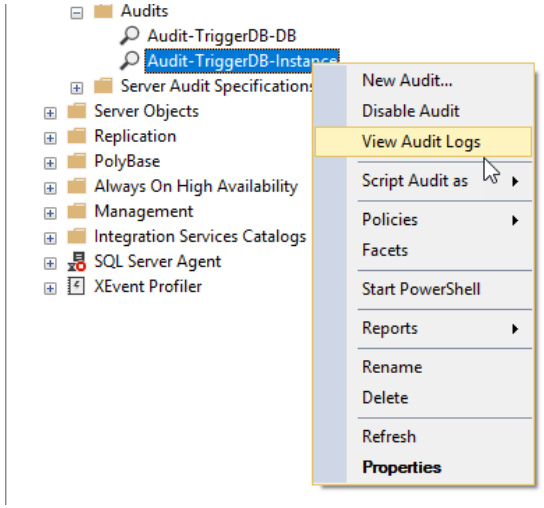
- Permite auditar eventos a nivel instancia.
- Permisos: ALTER ANY SERVER AUDIT , CONTROL SERVER or SYSADMIN
- https://docs.microsoft.com/es-mx/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15

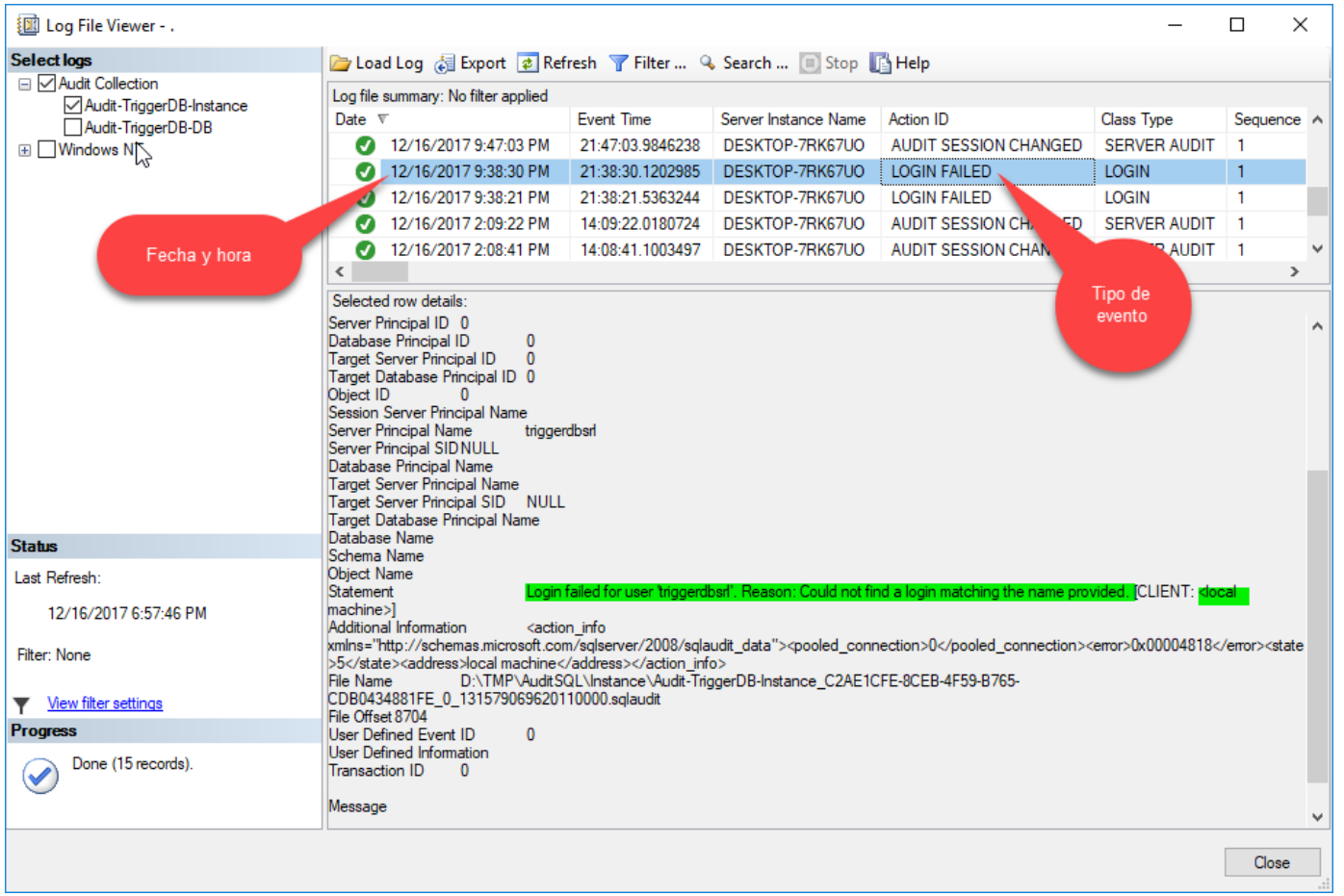
Database Audit Specification



- Permite auditar eventos a nivel base de datos.
- Permisos: ALTER ANY DATABASE AUDIT , CONTROL SERVER o SYSADMIN
- https://docs.microsoft.com/es-mx/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15

Registros de auditoria





- Se los pude ver desde SSMS o TSQL

Ver registros de auditoria TSQL

```
DECLARE @PATH VARCHAR(1024)
SELECT @PATH = LOG_FILE_PATH + '*.*'
FROM sys.server_file_audits
WHERE name = 'Audit-TriggerDB-Instance'

SELECT A.NAME,
       A.class_desc,
           A.parent_class_desc,
           A.covering_parent_action_name,
F.*
FROM sys.fn_get_audit_file
(@PATH,default,default) as F
left join sys.dm_audit_actions A
on F.action_id = A.action_id
ORDER BY EVENT_TIME DESC;
```

DEMOS

Muchas Gracias

Maximiliano Accotto
Owner **Triggerdb SRL**
Especialista en plataforma de datos Microsoft.
Microsoft MVP 2005-2019

POWER BI PARTNER

Microsoft Silver Partner

@maxiaccotto
https://ar.linkedin.com/in/maxiaccotto
https://blogs.triggerdb.com
maxi@triggerdb.com