

## GUIA: AUDITORIAS SQL SERVER PASO A PASO

Fecha: 22-02-2019

Autor: Maximiliano D. Accotto





## Derechos de autor

La información contenida en este documento representa la visión actual de **TriggerDB Consulting** sobre los problemas discutidos a la fecha de publicación. Debido a que **TriggerDB Consulting** debe responder a las cambiantes condiciones del mercado, no debe interpretarse como un compromiso por parte de **TriggerDB Consulting**, y **TriggerDB Consulting** no puede garantizar la exactitud de la información presentada después de la fecha de publicación.

Este documento técnico es solo para fines informativos. **TriggerDB Consulting** NO OTORGA NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA O ESTATUTARIA, CON RESPECTO A LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO.

El cumplimiento de todas las leyes de copyright aplicables es responsabilidad del usuario. Sin limitar los derechos protegidos por derechos de autor, ninguna parte de este documento puede reproducirse, almacenarse o introducirse en un sistema de recuperación, ni transmitirse de ninguna forma ni por ningún medio (electrónico, mecánico, fotocopia, grabación u otro), o por cualquier propósito, sin el permiso expreso por escrito de **TriggerDB Consulting**.

**TriggerDB Consulting** puede tener patentes, solicitudes de patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual que cubran el contenido de este documento. Salvo que se indique expresamente en cualquier acuerdo de licencia por escrito de **TriggerDB Consulting**, el suministro de este documento no le otorga ninguna licencia sobre estas patentes, marcas comerciales, derechos de autor u otra propiedad intelectual.





## ACERCA DEL AUTOR



Maximiliano Accotto es el fundador y CEO de TriggerDB Consulting SRL http://www.triggerdb.com

Se especializa como arquitecto, consultor y coach en los productos de Microsoft Data Platform (SQL Server, Big Data, Powerbi, BI, etc).

Desde el año 1997 trabaja como consultor en SQL Server donde he participado de distintos proyectos para más de 300 empresas de América y Europa, cubriendo todo lo relacionado a SQL Server y BI.

Desde el año 2005 es reconocido por Microsoft como MVP en SQL Server donde he recibido más de 12 premios.

Participa como orador de SQL Server desde el año 2003 donde ha impartido más de 200 conferencias a nivel mundial, entre ellas (Lanzamientos de SQL, eventos para comunidades y universidades, webinars y otros tantos más)

<u>https://twitter.com/maxiaccotto</u>

https://www.linkedin.com/in/maxiaccotto/





Microsoft Partner Silver Data Platform Silver Data Analytics

## 2 INTRODUCCION

En el área de seguridad informática es necesario en muchos casos poder contar con una auditorias de las operaciones que suceden en el motor de base de datos.

En esta guía vamos a ver paso a paso como se implementan las auditorias nativas que tiene SQL Server desde su versión 2008 o superior (<u>https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine</u>)

Debemos mencionar que para usar todas las funcionalidades de auditoria se requiere edición Enterprise de SQL Server ya que la Standard tiene la funcionalidad, pero de forma limitada.



## 3 COMPONENTES

Las auditorias contienen los siguientes componentes que describimos a continuación

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





Microsoft Partner

# Server Audit

Server Audit Specification

Database Audit Specification







## 4 PASO 1: SERVER AUDIT

El primer paso es crear los SERVER AUDIT, en ellos se podrá definir la persistencia y otras configuraciones adicionales.

En la guía crearemos dos Server Audit (uno para los eventos de instancia y otro para los de base de datos)

#### 4.1 PERMISOS DE SEGURIDAD

- Para crear, modificar o quitar una auditoría de servidor, las entidades de seguridad deben tener el permiso ALTER ANY SERVER AUDIT o CONTROL SERVER.
- Los usuarios con el permiso ALTER ANY SERVER AUDIT pueden crear especificaciones de auditoría de servidor y enlazarlas a cualquier auditoría.
- Una vez creada una especificación de auditoría de servidor, las entidades de seguridad que cuenten con los permisos CONTROL SERVER o ALTER ANY SERVER AUDIT, así como la cuenta sysadmin, o las entidades de seguridad que tengan acceso explícito a la auditoría podrán ver dicha especificación.

#### 4.2 CREAR SERVER AUDIT PARA EVENTOS DE INSTANCIA





| 😾 Create Audit   |  |   |                                       | _      |    | ×      |
|--|--|---|---------------------------------------|--------|----|--------|
| 🚺 Ready  |  |   |                                       |        |    |        |
| Select a page  | 🗐 Script 👻 😯 Hel   | p   |                                       |        |    |        |
| ≱ General<br>≱ Filter                                  | Audit name:<br>Queue delay (in<br>milliseconds):<br>On Audit Log<br>Failure: | Audit-TriggerDB-li<br>1000<br>Continue<br>Shut down see | nstance                               |        |    |        |
|  | Audit<br>destination:<br>File path:<br>Audit File<br>Maximum Limit:          | File D:\TMP\AuditSQ Maximum rollo Maximum files         | L\Instance<br>ver files:<br>Unlimited |        |    | ~      |
|  | Maximum file<br>size:<br>□ Reserve disk                                      | Number of files:  | 2147483647                            | ● GB   | 01 | ÷<br>B |
| Connection   |  |   |                                       |        |    |        |
| ↓ [DESKTOP-7RK67UO\maxi]<br>View connection properties |  |   |                                       |        |    |        |
|  |  |   |                                       |        |    |        |
| A Ready  |  |   |                                       |        |    |        |
|  |  |   | ОК                                    | Cancel | He | p      |

Microsoft

Silver Data Platform Silver Data Analytics

Audit Name Aquí debemos escribir el nombre del Server Audit, en nuestro caso Audit-TriggerDB-Instance ya que aquí solo la usaremos para eventos de instancia y no base de datos. Si bien se puede crear un solo archivo para todo, en nuestra experiencia es más ordenado tener dos o más Server Audit, separando los de instancia de los de base de datos 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). El máximo es 2.147.483.647 (2.147.483,647 segundos, o 24 días, 20 horas, 31 minutos y 23,647 segundos). **On Audit Log Failure Continue:** SQL Server 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, con lo que se infringirían las directivas de seguridad. Seleccione esta opción cuando la operación de continuación del Motor de base de datos sea más importante que el mantenimiento de una auditoría completa. 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 en el destino de la auditoría. Para poder usarlo, es preciso utilizar un inicio de sesión con el permiso SHUTDOWN. Si el inicio de sesión no tiene dicho permiso, la función generará un error y se mostrará un mensaje de error. No se producirán eventos auditados. 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. No se producirán 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: El destino serán archivos binarios<br>Security Log: Los eventos se escriben en el Security Log de Windows<br>Application Log: Los eventos se escriben en el Application Log de Windows |
|-------------------|--|
|                   | Nota: para todos los casos la cuenta de servicio del engine debe tener los permisos adecuados ya sea para escribir en las carpetas o en los eventos del SO                                   |
| File path         | La ruta donde se guardarán los archivos, en nuestro primer ejemplo hemos seleccionado<br>"D:\TMP\AuditSQL\Instance" ya que ahí guardaremos los archivos para los eventos de instancia        |
| Maximum file Size | Por defecto esta opción deja tener tamaño ilimitado, en nuestra guía y en base a nuestra experiencia configuraremos que los archivos no puedan tener más de 2GB cada uno                     |



El siguiente código TSQL es la representación de lo que hemos hecho anteriormente

```
USE [master]
GO
CREATE SERVER AUDIT [Audit-TriggerDB-Instance]
TO FILE
       FILEPATH = N'D:\TMP\AuditSQL\Instance'
(
       ,MAXSIZE = 2 GB
       ,MAX_ROLLOVER_FILES = 2147483647
       ,RESERVE_DISK_SPACE = OFF
)
WITH
       QUEUE_DELAY = 1000
(
       , ON_FAILURE = CONTINUE
)
GO
ALTER SERVER AUDIT [Audit-TriggerDB-Instance]
WITH (STATE = ON);
```



## 4.3 CREAR SERVER AUDIT PARA EVENTOS DE BASE DE DATOS











```
USE [master]
GO
CREATE SERVER AUDIT [Audit-TriggerDB-DB]
TO FILE
       FILEPATH = N'D:\TMP\AuditSQL\Databases'
(
       ,MAXSIZE = 2 GB
       ,MAX ROLLOVER FILES = 2147483647
       ,RESERVE_DISK_SPACE = OFF
)
WITH
(
       QUEUE_DELAY = 1000
       ,ON_FAILURE = CONTINUE
)
GO
ALTER SERVER AUDIT [Audit-TriggerDB-DB]
WITH (STATE = ON);
```



## 5 PASO 2: SERVER AUDIT SPECIFICATION

En este paso vamos a crear un Server Audit Specification para así poder auditar los eventos que nos interesa a nivel instancia.

En el siguiente link se encuentran los distintos eventos que se pueden auditar a nivel instancia y asignarlos al Server Audit Specification

https://docs.microsoft.com/es-mx/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions

#### 5.1 PERMISOS DE SEGURIDAD

- Para crear, modificar o quitar una auditoría de servidor, las entidades de seguridad deben tener el permiso ALTER ANY SERVER AUDIT O CONTROL SERVER.
- Los usuarios con el permiso ALTER ANY SERVER AUDIT pueden crear especificaciones de auditoría de servidor y enlazarlas a cualquier auditoría.
- Una vez creada una especificación de auditoría de servidor, las entidades de seguridad que cuenten con los permisos CONTROL SERVER o ALTER ANY SERVER AUDIT, así como la cuenta sysadmin, o las entidades de seguridad que tengan acceso explícito a la auditoría podrán ver dicha especificación.

#### 5.2 CREANDO SERVER AUDIT SPECIFICATION







| 灵 Create Server Audit Specificatio | 😥 Create Server Audit Specification — 🗆 🗙 |         |                             |                           |        |              |        | ×             |             |             |      |        |
|------------------------------------|---|---------|-----------------------------|---------------------------|--------|--------------|--------|---------------|-------------|-------------|------|--------|
| ) Ready                            |   |         |                             |                           |        |              |        |               |             |             |      |        |
| Select a page                      | 🛄 So                                      | cript   | 🕶 😮 Help                    |                           |        |              |        |               |             |             |      |        |
| 🔑 General                          |   |         |                             |                           |        |              |        |               |             |             |      |        |
|                                    | N   | lame:   | Server                      | rAuditSpecification-trigg | erdb   | 1            |        |               |             |             |      |        |
|                                    | A   | udit:   | Audit-                      | TriggerDB-Instance        |        |              |        |               |             |             |      | $\sim$ |
|                                    | A   | ctions: |                             |                           |        |              |        |               |             |             |      |        |
|                                    |   |         | Audit Action Type           | e                         |        | Object Class |        | Object Schema | Object Name | Principal I | Name |        |
| Connection                         |   | ▶1      | FAILED_LOGIN_GROUP          |                           | ~      |              | $\sim$ |               |             |             |      |        |
| ₩ . [DESKTOP-7RK67UO\maxi]         |   | 2       | LOGIN_CHANGE_PASSWORD_GROUP |                           | ~      |              | ~      |               |             |             |      |        |
|                                    |   | *3      |                             |                           | $\sim$ |              | $\sim$ |               |             |             |      |        |
|                                    |   |         |                             |                           |        |              |        |               |             |             |      |        |
| View connection properties         |   |         |                             |                           |        |              |        |               |             |             |      |        |
| Progress                           |   |         |                             |                           |        |              |        |               |             |             |      |        |
| Ready                              |   |         |                             |                           |        |              |        |               |             |             |      |        |
|                                    |   |         |                             |                           |        |              |        |               |             |             |      |        |
|                                    |   |         |                             |                           |        |              |        |               | ОК          | Cancel      | He   | lp     |

NameAquí ingresaremos el nombre de nuestro Server Audit Specification , en nuestro ejemplo<br/>"ServerAuditSpecification-triggerdb"AuditAquí debemos seleccionar el Server Audit en el cual se persistirán los eventos (los hemos<br/>creado en el paso anterior) , en nuestro ejemplo usaremos "Audit-TriggerDB-Instance"ActionsAquí seleccionaremos los eventos a auditar, para este ejemplo solo hemos elegido dos

| Security Constraints Server Roles Server Roles Credentials Credentials Cryptographic Provid Audits P Audit-Trigge Audit-Trigge Audit-Trigge | ers<br>New Server Audit Specification     |
|---|---|
| Server Audit Spe     Image: Server Audit Spe  | Script Server Audit Specification         |
| Server Objects     PolyEase     PolyBase     PolyBase     Management     Integration Services     B. SQL Server Agent                       | Policies  Facets Start PowerShell Reports |
| Ready   | Delete<br>Refresh<br>Properties           |

USE [master] GO CREATE SERVER AUDIT SPECIFICATION [ServerAuditSpecification-triggerdb] FOR SERVER AUDIT [Audit-TriggerDB-Instance] ADD (FAILED\_LOGIN\_GROUP), ADD (LOGIN\_CHANGE\_PASSWORD\_GROUP) GO ALTER SERVER AUDIT SPECIFICATION [ServerAuditSpecification-triggerdb] WITH (STATE = ON);





## 6 PASO 3: DATABASE AUDIT SPECIFICATION

A diferencia del Server Audit Specification, los Database Audit Specification se deben crear por cada una de las bases de datos que se desee auditar.

Este objeto reside en la metada de la base de datos con lo cual un Backup / Restore también incluirá estas definiciones.

#### 6.1 PERMISOS DE SEGURIDAD

- Los usuarios con el permiso ALTER ANY DATABASE AUDIT pueden crear las especificaciones de auditoría de base de datos y enlazarlas a cualquier auditoría.
- Después de crearse una especificación de auditoría de base de datos, podrá ser vista por las entidades de seguridad que cuenten con los permisos CONTROL SERVER o ALTER ANY DATABASE AUDIT, o por la cuenta sysadmin

#### 6.2 ALGUNAS RECOMENDACIONES

En la mayoría de las empresas lo que se desea auditar (sobre todo a nivel base de datos) son las operaciones realizadas por usuarios fuera de las aplicaciones de gestión. Un ejemplo, seria poder capturar un UPDATE o un SELECT de un usuario utilizando herramientas como Management Studio, Excel, etc.

A tal fin y en base a nuestra experiencia implementando auditorias en varias empresas es que aconsejamos aplicar un filtro de que usuarios vamos a realmente auditar así luego nuestro log no se llena con eventos que quizás nunca veremos.

Para hacer esta operación hay dos formas posibles que luego veremos a continuación a lo largo de esta guía.

#### 6.3 CREAR DATABASE AUDIT SPECIFICATION

Esta operación la haremos sobre la base de datos que deseamos auditar, en nuestro ejemplo usaremos "AdventureWorks2014"







| 灵 Create Database Audit Specifica | tion       |          |           |                                       |      |              |        |               |                    | - 0            | ×           |
|-----------------------------------|------------|----------|-----------|---------------------------------------|------|--------------|--------|---------------|--------------------|----------------|-------------|
| Ready                             |            |          |           |                                       |      |              |        |               |                    |                |             |
| Select a page                     | <b>J</b> : | Script   | 🕶 😧 Help  |                                       |      |              |        |               |                    |                |             |
|                                   |            | Name:    |           | DatabaseAuditSpecification            | n-Ti | riggerDB     |        |               |                    |                |             |
|                                   |            | Audit:   |           | Audit-TriggerDB-DB                    |      |              |        |               |                    |                | ~           |
|                                   |            | Actions: |           |                                       |      |              |        |               |                    |                |             |
|                                   | [          |          | Audit Act | ion Type                              |      | Object Class | 3      | Object Schema | Object Name        | Principal Name |             |
| Connection                        |            | 1        | SELECT    |                                       | ~    | DATABASE     | $\sim$ |               | AdventureWorks2014 | <br>public     |             |
| v₩ . [DESKTOP-7RK67UO\maxi]       |            | 2        | UPDATE    |                                       | ~    | DATABASE     | $\sim$ |               | AdventureWorks2014 | <br>public     |             |
|                                   |            | ▶ 3      | DELETE    |                                       | ~    | DATABASE     | $\sim$ |               | AdventureWorks2014 | <br>public     |             |
|                                   |            | *4       |           | · · · · · · · · · · · · · · · · · · · | ~    |              | $\sim$ |               |                    |                |             |
| View connection properties        |            |          |           |                                       |      |              |        |               |                    |                |             |
| Progress                          |            |          |           |                                       |      |              |        |               |                    |                |             |
| Ready                             |            |          |           |                                       |      |              |        |               |                    |                |             |
|                                   |            |          |           |                                       |      |              |        |               |                    |                |             |
|                                   |            |          |           |                                       |      |              |        |               | ОК                 | Cancel H       | Help<br>.:: |

| Name(*)               | Aquí ingresaremos el nombre de nuestro Database Audit Specification , en nuestro ejemplo<br>"DatabaseAuditSpecification-TriggerDB"   |
|-----------------------|--|
| Audit(*)              | Aquí debemos seleccionar el Server Audit en el cual se persistirán los eventos. En nuestro ejemplo seleccionamos "Audit-TriggerDB-DB" ya que hemos divido los eventos de servidor de los de base de datos en dos Server Audit distintos.   |
| Audit Action Type (*) | Aquí seleccionaremos los eventos a auditar. En el siguiente link se encuentra el listado de todos los eventos disponibles<br>https://docs.microsoft.com/es-mx/sql/relational-databases/security/auditing/sql-server-<br>audit-action-groups-and-actions  |
| Object Class(*)       | Aquí debe seleccionar el tipo de objeto a auditar donde las opciones son:<br><b>Database:</b> Se auditarán todos los objetos de la base de datos<br><b>Object:</b> Solo se auditará el objeto seleccionado (por ejemplo, una tabla en particular)<br><b>Schema:</b> Se auditarán los objetos que estén dentro del schema (por ejemplo, DBO)  |
| Object Schema         | Si se selecciona en object class auditar un schema, en este campo deberá indicar cuál.   |
| Object Name           | Debe indicar el nombre del objeto a auditar ya sea para Database u Object. En nuestro caso hemos seleccionado Adventureworks2014 que es el nombre de la base de datos  |
| Principal Name(*)     | Aquí debe elegir un Database Role, un usuario o un Application Role.<br>En nuestro ejemplo hemos seleccionado al role Public , lo cual indica que auditaremos a todos los usuarios.<br>Si desea no auditar a los usuarios de la aplicación y si a los externos, una alternativa seria crear un role en cada base de datos (por ejemplo, llamado Auditoria) y seleccionar ese role en principal name (en lugar del public)<br>Si además desea auditar a los Sysadmin de su servidor (estos por lo general no son ni usuarios de sus bases de datos) debería agregar a los mismos eventos el role dbo (como se muestra en la figura siguiente) |
|                       |  |

## \*Campos obligatorios



| Image: Progress         Progres         Progres         Progre  | 疑 Create Database Audit Specific | ation          |          |                        |        |             |        |               |                    | _              |   | > |
|--|----------------------------------|----------------|----------|------------------------|--------|-------------|--------|---------------|--------------------|----------------|---|---|
| Select a page  | 🕕 Ready                          |                |          |                        |        |             |        |               |                    |                |   |   |
| ✓ General       Name:       DatabaseAudttSpecification-TriggerDB         Audit:       Audit-TriggerDB-DB       Audit-TriggerDB-DB         Actions:       Actions:         Connection       1       SELECT       > DATABASE       AdventureWorks2014       public          1       SELECT       > DATABASE       AdventureWorks2014        public          2       UPDATE       > DATABASE       AdventureWorks2014        public          3       DELETE       > DATABASE       AdventureWorks2014        public          4       SELECT       > DATABASE       AdventureWorks2014        public          5       UPDATE       > DATABASE       AdventureWorks2014        dba          6       DELETE       > DATABASE       AdventureWorks2014        dba          6       DELETE       > DATABASE       AdventureWorks2014        dba          7   | Select a page                    | Script         | 🕶 😯 Help |                        |        |             |        |               |                    |                |   |   |
| Name: DatabaseAudit Specification-TriggerDB   Audit: Audit-TriggerDB-DB   Audit: Audit-TriggerDB-DB   Actions:     Connection         Audit Action Type   Object Class   Object Name    Principal Name         SELECT        UPDATE        DELETE           SELECT       DATABASE   AdventureWorks2014       UPDATE   DATABASE   AdventureWorks2014   Database   Database <td>👂 General</td> <td></td>  | 👂 General                        |                |          |                        |        |             |        |               |                    |                |   |   |
| Audit:       Audit.TriggerDB-DB <ul> <li>Audit.TriggerDB-DB</li> <li>Audit.TriggerDB-DB</li> </ul> Connection       Audit.Action Type       Object Class       Object Schema       Object Name       Principal Name <ul> <li>Principal Name</li> <li>SELECT</li> <li>DATABASE</li> <li>AdventureWorks2014</li> <li>public</li> <li>public</li></ul>  |                                  | <u>N</u> ame:  |          | DatabaseAuditSpecifica | ion-1  | [riggerDB   |        |               |                    |                |   |   |
| Actions:         Connection       Midt Action Type       Object Class       Object Schema       Object Name       Principal Name         1       SELECT       DATABASE       AdventureWorks2014       public          2       UPDATE       DATABASE       AdventureWorks2014       public          3       DELETE       DATABASE       AdventureWorks2014       public          4       SELECT       DATABASE       AdventureWorks2014       dbo          5       UPDATE       DATABASE       AdventureWorks2014       dbo          5       UPDATE       DATABASE       AdventureWorks2014        dbo          6       DELETE       DATABASE       AdventureWorks2014        dbo          7       Intervention       DATABASE       AdventureWorks2014        dbo  |                                  | <u>A</u> udit: |          | Audit-TriggerDB-DB     |        |             |        |               |                    |                |   | ~ |
| Connection       Number of the second |                                  | Actions        | 3:       |                        |        |             |        |               |                    |                |   |   |
| Connection       1       SELECT       DATABASE       AdventureWorks2014       public          2       UPDATE       DATABASE       AdventureWorks2014       public          3       DELETE       DATABASE       AdventureWorks2014        public          4       SELECT       DATABASE       AdventureWorks2014        public          5       UPDATE       DATABASE       AdventureWorks2014        dbo          6       DELETE       DATABASE       AdventureWorks2014        dbo          7       UPDATE       DATABASE       AdventureWorks2014        dbo          8       DELETE       DATABASE       DATABASE       AdventureWorks2014        dbo          9       DeleTE       DATABASE       DATABASE       AdventureWorks2014        dbo          9       DeleTE       DATABASE       DATABASE       AdventureWorks2014        dbo          9       Done       Done       DATABASE       Notesta   |                                  |                | 4        | Audit Action Type      | -      | Object Clas | s      | Object Schema | Object Name        | Principal Name | ; |   |
| <sup>1</sup> (DESKTOP-7RK67U0\maxi) <sup>2</sup> UPDATE <sup>3</sup> DELETE <sup>4</sup> SELECT <sup>5</sup> UPDATE <sup>6</sup> DELETE <sup>6</sup> DELETE <sup>6</sup> OELETE  | Connection                       | 1              | SELECT   |                        | ~      | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>public     |   |   |
| Mew connection properties       3       DELETE   | IDESKTOP-7RK67UO\maxi            | 2              | UPDATE   |                        | ~      | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>public     |   |   |
| View connection properties       4       SELECT       DATABASE       AdventureWorks2014       dbo          5       UPDATE       DATABASE       AdventureWorks2014        dbo          6       DELETE       DATABASE       AdventureWorks2014        dbo          • 7   |                                  | 3              | DELETE   |                        | $\sim$ | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>public     |   |   |
| View connection properties       5       UPDATE       DATABASE       AdventureWorks2014       dbo          Progress       6       DELETE       DATABASE       DATABASE       AdventureWorks2014        dbo          * 7       7       * <t< td=""><td></td><td>4</td><td>SELECT</td><td></td><td><math>\sim</math></td><td>DATABASE</td><td><math>\sim</math></td><td></td><td>AdventureWorks2014</td><td><br/>dbo</td><td></td><td></td></t<>   |                                  | 4              | SELECT   |                        | $\sim$ | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>dbo        |   |   |
| Progress     > 6     DELETE     > DATABASE     AdventureWorks2014     dbo       •7     •7     •     •     •  | View connection properties       | 5              | UPDATE   |                        | $\sim$ | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>dbo        |   |   |
| Done 47 V V V  | Progress                         | ▶ 6            | DELETE   |                        | $\sim$ | DATABASE    | $\sim$ |               | AdventureWorks2014 | <br>dbo        |   |   |
|  | Done                             | •7             |          |                        | $\sim$ |             | $\sim$ |               |                    |                |   |   |
|  | $\checkmark$                     |                |          |                        |        |             |        |               |                    |                |   |   |
|  |                                  |                |          |                        |        |             |        |               |                    |                |   |   |



USE [AdventureWorks2014] GO

CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification-TriggerDB] FOR SERVER AUDIT [Audit-TriggerDB-DB] ADD (SELECT ON DATABASE::[AdventureWorks2014] BY [public]), ADD (UPDATE ON DATABASE::[AdventureWorks2014] BY [public]), ADD (DELETE ON DATABASE::[AdventureWorks2014] BY [public]), ADD (SELECT ON DATABASE::[AdventureWorks2014] BY [public]), ADD (SELECT ON DATABASE::[AdventureWorks2014] BY [dbo]), ADD (UPDATE ON DATABASE::[AdventureWorks2014] BY [dbo]),





Microsoft Silver Data Platform Partner Silver Data Analytics

ADD (DELETE ON DATABASE::[AdventureWorks2014] BY [dbo]) WITH (STATE = ON) GO

## 7 FILTRAR REGISTROS EN EL SERVER AUDIT

Como hemos comentado anteriormente en este documento, en la auditoria quizás no tenga sentido que se registren los eventos provenientes de las aplicaciones de gestión y si de las externas.

Al crear el Database Audit Specification hemos visto que podríamos resolver esto creando un role en la base de datos y luego asignando a los usuarios que debemos auditar en dicho role , seria técnicamente como poderlos agrupar de alguna forma.

En esta sección veremos una segunda técnica que directamente aplica al Server Audit y es la posibilidad de filtrar ahí mismo sin importar de donde se haga el evento.

Este método si tenemos muchas bases de datos quizás es mejor que el anterior ya que nos permite mejorar la administración.

Tenga cuidado si por ejemplo desea auditar eventos en el Server Audit Specification como SUCCESFUL\_LOGIN\_GROUP y otros eventos más en la misma especificación, si filtra los de la aplicación estará perdiendo de datos. Imagine que desea auditar login sucess y cambios de clave y no le interesa ver en su auditoria los de login sucess que sean del login de la aplicación (le llenera el log seguramente y esa información es probable que no sea relevante para un departamento de seguridad informática).

Para resolver este ultima caso lo que usted debería hacer es crear dos Server Audit distintos (uno con filtro y el otro no) y dos Server Audit Specification distintos (por ejemplo, los eventos de Successful\_login\_group en uno y en el otro el resto)

Para aplicar los filtros sobre un Server Audit ya existente se deben seguir los siguientes pasos

1. Poner en disable el Server Audit





#### 2. Agregar al Server Audit el filtro

| Audit Properties                         | _   |     | $\times$ |
|--|---|-----|----------|
| 🕕 Ready                                  |   |     |          |
| Select a page<br>∦ General<br>∦ Filter   | Script  Help  ([server_principal_name]<>'sql1' AND [server_principal_name]<>'sql2') |     | ^        |
| Connection<br>y∰ .[DESKTOP-7RK67UO\maxi] |   |     |          |
| View connection properties               |   |     |          |
| Ready                                    |   |     | ~        |
|  | OK Cancel   | Hel | p        |

3. Volver a habilitar el Server Audit







```
ALTER SERVER AUDIT [Audit-TriggerDB-DB]
WITH (STATE = OFF)
GO
USE [master]
GO
ALTER SERVER AUDIT [Audit-TriggerDB-DB]
WHERE ([server_principal_name]<>'sql1'
AND [server_principal_name]<>'sql2')
GO
ALTER SERVER AUDIT [Audit-TriggerDB-DB]
WITH (STATE = ON)
```

Nota: en este ejemplo hemos seleccionado el Server Audit que hemos creado para persistir los eventos de base de datos y le hemos agregado el filtro para que excluya a los login SQL1 y SQL2

#### 8 VER LOS RESULADOS DE LA AUDITORIA

Para poder ver los distintos eventos con su correspondiente detalle existen dos alternativas que veremos a continuación.

#### 8.1 USANDO EL SQL SERVER MANAGEMENT STUDIO (SSMS)

Desde el propio SSMS se pueden ver los registros del log, para eso lo que se debe hacer es lo siguiente sobre el Server Audit que deseamos observar





|  |   |   |   |   | -  |  | ×     |
|--|---|---|---|---|--|--|-------|
| Selectlogs   | 📄 🗁 Load Log 👌 Export 🛛 🐼 Re  | fresh 🍸 Filter 🤇  | 💊 Search 🔳 Stop 🚦   | 🖪 Help  |  |  |       |
| Audit Collection   | Log file summary: No filter applied   |   |   |   |  |  |       |
| Audit-TriggerDB-Instance   | Date V  | Event Time  | Server Instance Name  | Action ID   | Class Type   | Seque  | nce 🗠 |
| Windows NT   | 12/16/2017 9:47:03 PM   | 21:47:03.9846238  | DESKTOP-7RK67UO   | AUDIT SESSION CHANGED   | SERVER AUDIT   | 1  |       |
|  | 12/16/2017 9:38:30 PM   | 21:38:30.1202985  | DESKTOP-7RK67UO   | LOGIN FAILED  | LOGIN  | 1  |       |
|  | 12/16/2017 9:38:21 PM   | 21:38:21.5363244  | DESKTOP-7RK67UO   | LOGIN FAILED  | LOGIN  | 1  | - 1   |
|  | 12/16/2017 2:09:22 PM   | 14:09:22.0180724  | DESKTOP-7RK67UO   | AUDIT SESSION CH. FD  | SERVER AUDIT   | 1  |       |
| Eacha y bara   | 12/16/2017 2:08:41 PM   | 14:08:41.1003497  | DESKTOP-7RK67UO   | AUDIT SESSION CHAN  | R AUDIT  | 1  | ~     |
| r echa y hora  | <   |   |   |   |  |  | >     |
|  | Server Principal ID 0<br>Database Principal ID 0<br>Target Server Principal ID 0<br>Target Database Principal ID 0<br>Object ID 0<br>Session Server Principal Name<br>Server Principal Name trigge  | rdbsrl  |   |   | evento   |  | ^     |
|  | Server Principal SIDNULL<br>Database Principal Name<br>Target Server Principal Name<br>Target Server Principal SID NULL<br>Target Database Principal Name   |   |   |   |  |  | l     |
| Status   | Server Principal SIDNULL<br>Database Principal Name<br>Target Server Principal Name<br>Target Server Principal SID NULL<br>Target Database Principal Name<br>Database Name  |   |   |   |  |  | 1     |
| Status<br>Last Refresh:  | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal Name<br>Target Server Principal SID NULL<br>Target Database Principal Name<br>Database Name<br>Object Name  |   |   |   |  |  |       |
| Status<br>Last Refresh:<br>12/16/2017 6:57:46 PM<br>Filter: None   | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal SID NULL<br>Target Server Principal SID NULL<br>Target Database Principal Name<br>Database Name<br>Schema Name<br>Object Name<br>Statement Communications<br>Object Name<br>Statement Communications<br>Object Name<br>Statement Communications<br>Statement Co | f <b>ailed for user hipperd</b><br>on_info<br>m/sqlserver/2008/sqla<br>//address> <td>bsti Reason Could not fit<br/>sudit_data"&gt;<ppcoled_conr<br>fo&gt;</ppcoled_conr<br></td> <td>nd a login matching the name pro<br/>hection&gt;0</td> <td>vided [CLIENT: doc</td> <td>2<b>al</b><br/>/error&gt;<s< td=""><td>state</td></s<></td>  | bsti Reason Could not fit<br>sudit_data"> <ppcoled_conr<br>fo&gt;</ppcoled_conr<br>                                     | nd a login matching the name pro<br>hection>0                         | vided [CLIENT: doc   | 2 <b>al</b><br>/error> <s< td=""><td>state</td></s<> | state |
| Status<br>Last Refresh:<br>12/16/2017 6:57:46 PM<br>Fitter: None   | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal Name<br>Database Principal Name<br>Database Name<br>Schema Name<br>Schema Name<br>Schema Name<br>Cateria Cateria<br>Nationes<br>Additional Irformation caciti<br>xmina-"http://schemas.microsoft.co<br>25/s/data-zadiress/local machines<br>File Name<br>District Machines 115/570695020  | -<br>failed for user Niggerd<br>on_info<br>//address>//action_inf<br>/QL\Instance\Audit_Tin<br>10000.sqlaudit   | bel Reason Could not fo<br>sudit data"> <pooled_com<br>io&gt;<br/>ggerDB-Instance_C2AE10</pooled_com<br>                | nd a logn matching the name pro<br>vection>0<br>FE-80CEB-4F59-8765-   | vided CLIENT: doc<br><emor>0x00004818<!--</td--><td>c<b>al</b><br/>/error&gt;<s< td=""><td>state</td></s<></td></emor> | c <b>al</b><br>/error> <s< td=""><td>state</td></s<> | state |
| Status<br>Last Refresh:<br>12/16/2017 6:57:46 PM<br>Filter: None<br>Y Wew filter settings<br>Progress                      | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal SID NULL<br>Target Server Principal SID NULL<br>Target Database Nicopal Name<br>Schema Name<br>Object Name<br>Statement<br>machine/It/mation cactio<br>mrins-Thtp://schemas.microsoft.co<br>SiC/state>caddress/bocil machine<br>Distributional information<br>cabled:48.081Fc.013673062001<br>Re: Offset 8704   | -<br>failed for user Niggerd<br>on_info<br>m/salpserver/2008/sqla<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf<br>/address-2-adion_inf | bart Reason: Could not fa<br>sudit_data"> <pooled_com<br>fo<br/>ggerDB-instance_C2AE1(</pooled_com<br>                  | nd a login matching the name pro<br>nection>0+<br>:FE-8CEB-4F59-B765- | vided CLIENT: doc<br><error>0x00004818<!--</td--><td>sat<br/>/error&gt;<s< td=""><td>state</td></s<></td></error>      | sat<br>/error> <s< td=""><td>state</td></s<>         | state |
| Status<br>Last Refresh:<br>12/16/2017 6.57.46 PM<br>Filter: None<br>View filter settings<br>Progress<br>One (15 records).  | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal SID<br>NULL<br>Target Server Principal SID<br>Database Name<br>Schema Name<br>Object Name<br>Statement<br>machine>]<br>Additional Information caditi<br>winds-"Http://schemas.microsoft.co<br>p5/ct/atab <address local="" machine=""><br/>He Name<br/>Dittle Vatabase<br/>CDB043488/FE_0_1315790696207<br/>He Offred Event ID<br/>User Defined Event ID<br/>User Defined Information<br/>Transaction ID<br/>0</address>  | -<br><b>failed for user Inggerd</b><br>yn jafo<br>m/sglserver/2008/sgls<br>/sddress-/saction.jif<br>10000.sglaudit<br>10000.sglaudit  | bell Reason Could not for<br>audit, data"> <pooled_conr<br>to&gt;<br/>c&gt;<br/>ggerDB-Instance_C2AE10</pooled_conr<br> | nd a logn matching the name pro<br>nection>0<br>FFE-8CEB-4F59-B765-   | wided CLIENT: the  | cal<br>/error> <s< td=""><td>state</td></s<>         | state |
| Status<br>Last Refresh:<br>12/16/2017 6:57:46 PM<br>Filter: None<br>View filter settings<br>Progress<br>Done (15 records). | Server Principal SID NULL<br>Database Principal Name<br>Target Server Principal Name<br>Target Server Principal Name<br>Debabase Nimopal Name<br>Debabase Name<br>Object Name<br>Statement Locat<br>machine-J<br>Additional Irformation cactit<br>xmins-"http://schemas.microsoft.co<br>55/state-schdress/local machine-<br>File Name D-STMP-VudtS<br>CDB04/3481FE_0_1315790695201<br>File Offset 8704<br>User Defred Irformation<br>Transaction ID 0<br>Message  | -<br>failed for user Inggerd<br>m/aglerver/2008/agin<br>/address-vel/address-vel/addr<br>GU.Vnetance-Veudt Tri<br>10000.sqlaudit  | bat Reason. Could not fa<br>sudit_data"> <pooled_conr<br>io&gt;<br/>ggerDB-Instance_C2AE10</pooled_conr<br>             | nd a login matching the name pro<br>vection>0<br>:FE-8CEB-4F59-8765-  | vided_CLIENT: <mark>dor</mark><br><eror>0x00004818&lt;</eror>  | oal<br>∕error> <s< td=""><td>state</td></s<>         | state |

En esta última figura podemos observar que hubo un login fail y todo el detalle del mismo (fecha y hora, tipo de acción, etc)

Si hacemos el mismo procedimiento sobre el server Audit que alojamos los eventos de base de datos veremos los mismos atributos, pero obviamente con otros datos

| 🔟 Log File Viewer        |  |  |                        |                       | - 🗆        | $\times$ |
|--------------------------|--|--|------------------------|-----------------------|------------|----------|
| Selectlogs               | 📄 Load Log 🛛 🖓 Export 👔 Re   | efresh 🍸 Filter 🤇  | Search 🔳 Stop          | 📑 Help                |            |          |
|                          | Log file summary: No filter applied  |  |                        | - <u>-</u>            |            |          |
| Audit-TriggerDB-Instance | Date 🔻   | Event Time   | Server Instance Name   | Action ID             | Class Type | Ser      |
| Windows NT               | 12/16/2017 9:55:16 PM  | 21:55:16.2585454   | DESKTOP-7RK67UO        | SELECT                | TABLE      | 1        |
|                          | 12/16/2017 9:55:14 PM  | 21:55:14.5655393   | DESKTOP-7RK67UO        | SELECT                | TABLE      | 1        |
|                          | 12/16/2017 9:55:11 PM  | 21:55:11.8858452   | DESKTOP-7RK67UO        | AUDIT SESSION CHANGED | SERVER AUD | IT 1     |
|                          | <  |  |                        |                       |            | 3        |
|                          | Selected row details:  |  |                        |                       |            |          |
|                          | Date 12/16/2017 9:<br>Log Audit Collection   | 55:16 PM<br>n (Audit-TriggerDB-DB)   |                        |                       |            | ^        |
| Status                   | Server Instance Name DES<br>Action ID SELECT<br>Class Type TAB<br>Sequence Number 1<br>Succeeded True<br>Permission Bit Mask 0x00000000<br>Column Permission True<br>Session ID 68<br>Server Principal ID 1<br>Database Principal ID 1<br>Target Server Principal ID 0<br>Target Database Principal ID 0 | U000001  |                        |                       |            |          |
| Last Refresh:            | Session Server Principal Name  | sa   |                        |                       |            |          |
| 12/16/2017 7:08:43 PM    | Server Principal Name sa<br>Server Principal SID 0x1<br>Database Principal Name dho  |  |                        |                       |            |          |
| Filter: None             | Target Server Principal Name<br>Target Server Principal SID NUL  | L  |                        |                       |            |          |
| Y View filter settings   | Database Name AdventureWork  | ks2014   |                        |                       |            |          |
| Progress                 | Schema Name Sales  |  | _                      |                       |            |          |
| Done (3 records).        | Statement select<br>Additional Information<br>File Name D:\TMP\Audit:<br>496C066A50D5 0 131579349118   | <mark>t * from sales.Customer</mark><br>SQL∖Databases∖Audit- <sup>-</sup><br>700000.solaudit | TriggerDB-DB_611939FD· | F226-4AF2-A8B8-       |            |          |
|                          |  |  |                        |                       |            |          |
|                          |  |  |                        |                       | 0          |          |







## 8.2 USANDO CODIGO TSQL

Otra alternativa mucho más completa y customizada es poder usar código TSQL, esto nos permitirá entre varias cosas por ejemplo integrar o armar informes en herramientas como PowerBI, Excel, reporting Services, etc.

Para poder usar esta opción SQL Server dispone de una función llamada sys.fn\_get\_audit\_file (https://docs.microsoft.com/en-us/sql/relational-databases/system-functions/sys-fn-get-audit-file-transact-sql)

Con la cual podemos leer los archivos de auditoria y que el resultado sea una tabla para luego verlo o integrarlo con otras soluciones.

Con esta función y las vistas de SQL Server correspondientes a Audit se puede buscar toda la información necesaria

| svs server audits                        | Contiene una fila para cada auditoría de SOL Server de una instancia de  |
|--|--|
| sys.server_addres                        | servidor   |
|  | https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-server-   |
|  | audits-transact-sql  |
|  | Operation o informa ción o dicional colore al tino de conditería de continuo en un   |
| sys.server_file_audits                   | Contiene información adicional sobre el tipo de auditoria de archivos en un  |
|  | https://docs.microsoft.com/es-mx/sql/relational-databases/system-catalog-views/sys-server-file-                                      |
|  | audits-transact-sql  |
|  |  |
| sys.server_file_audits                   | Contiene información adicional sobre el tipo de auditoria de archivos en un  |
|  | SQL Server<br>https://docs.microsoft.com/es-mx/sql/relational-databases/system-catalog-views/sys-server-file-                        |
|  | audits-transact-sql  |
|  |  |
| sys.server_audit_specifications          | Contiene información sobre las especificaciones de auditoria de servidor de  |
|  | https://docs.microsoft.com/es-mx/sql/relational-databases/system-catalog-views/sys-server-audit-                                     |
|  | specifications-transact-sql  |
| ave conver audit exception details       | Contigno información achro los datallos de conocificación de auditoría del   |
| sys.server_audit_specification_details   | servidor (acciones)  |
|  | https://docs.microsoft.com/es-es/sql/relational-databases/system-catalog-views/sys-server-audit-                                     |
|  | specification-details-transact-sql   |
| sys database audit specifications        | Contiene información sobre las especificaciones de auditoría de base de datos  |
| systatusase_adate_specifications         | https://docs.microsoft.com/es-es/sql/relational-databases/system-catalog-views/sys-database-   |
|  | audit-specifications-transact-sql  |
| sys database audit specification details | Contiene información sobre las especificaciones de auditoría de base de datos  |
| systatubuse_duale_specification_details  | en una auditoría de SQL Server de una instancia de servidor para todas las   |
|  | bases de datos   |
|  | https://docs.microsoft.com/es-es/sql/relational-databases/system-catalog-views/sys-database-   |
|  |  |
| sys.dm_server_audit_status               | Devuelve una fila para cada auditoría de servidor que indica el estado actual  |
|  | de la misma  |
|  | mups.//docs.microsort.com/es-es/sql/relational-databases/system-dynamic-management-views/sys-<br>dm-server-audit-status-transact-sql |
|  |  |
| sys.dm_audit_actions                     | Devuelve una fila por cada acción de auditoría sobre la que se puede guardar   |
|  | informacion en el registro de auditoria y por cada grupo de acciones de  |
|  | https://docs.microsoft.com/es-es/sgl/relational-databases/system-dynamic-management-views/svs-                                       |
|  | dm-audit-actions-transact-sql  |
| sve de audit class turo man              | Devuelve una tabla que asigna el campo class, type del registro de auditoría al  |
| sys.un_auur_crass_type_map               | campo class desc en sys.dm audit actions   |
|  | https://docs.microsoft.com/es-es/sql/relational-databases/system-dynamic-management-views/sys-                                       |
|  | dm-audit-class-type-man-transact-sol   |





El siguiente código TSQL buscara todos los eventos de los archivos existentes para la auditoria "Audit-TriggerDB-Instance"

```
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;
```

GO

| I Results 👔 Messages |                       |              |                   |                             |                             |                 |           |           |  |
|----------------------|-----------------------|--------------|-------------------|-----------------------------|-----------------------------|-----------------|-----------|-----------|--|
|                      | NAME                  | class_desc   | parent_class_desc | covering_parent_action_name | event_time                  | sequence_number | action_id | succeeded | permission_bitmask                     |
| 1                    | LOGIN FAILED          | LOGIN        | SERVER            | FAILED_LOGIN_GROUP          | 2017-12-16 21:53:29.8367338 | 1               | LGIF      | 0         | 0x000000000000000000000000000000000000 |
| 2                    | LOGIN FAILED          | LOGIN        | SERVER            | FAILED_LOGIN_GROUP          | 2017-12-16 21:53:29.8327310 | 1               | LGIF      | 0         | 0x000000000000000000000000000000000000 |
| 3                    | LOGIN FAILED          | LOGIN        | SERVER            | FAILED_LOGIN_GROUP          | 2017-12-16 21:53:29.8327310 | 1               | LGIF      | 0         | 0x000000000000000000000000000000000000 |
| 4                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:53:16.1506885 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 5                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:53:00.5326848 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 6                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:53:00.5326848 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 7                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:47:54.1257572 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 8                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:47:03.9966316 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 9                    | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 21:47:03.9846238 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 10                   | LOGIN FAILED          | LOGIN        | SERVER            | FAILED_LOGIN_GROUP          | 2017-12-16 21:38:30.1202985 | 1               | LGIF      | 0         | 0x000000000000000000000000000000000000 |
| 11                   | LOGIN FAILED          | LOGIN        | SERVER            | FAILED_LOGIN_GROUP          | 2017-12-16 21:38:21.5363244 | 1               | LGIF      | 0         | 0x000000000000000000000000000000000000 |
| 12                   | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 14:09:22.0180724 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 13                   | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 14:08:41.1003497 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 14                   | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 14:08:41.0963504 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |
| 15                   | AUDIT SESSION CHANGED | SERVER AUDIT | SERVER            | NULL                        | 2017-12-16 14:08:37.7422663 | 1               | AUSC      | 1         | 0x000000000000000000000000000000000000 |





## 9 PERFORMANCE Y CONCLUSIONES

La utilización de eventos y asincronismo hacen que las implementaciones de las auditorias nativas no tengan impacto en la performance de nuestro motor como si suele suceder con otras técnicas como por ejemplo el uso de trigger.

Las auditorias están disponibles desde SQL Server 2008 lo cual la hacen una funcionalidad madura.

Si bien se pueden usar otros métodos de auditoria (extend Events y profiler entre otros) las auditorias nativas son robustas y contienen todo lo necesario para una implementación adecuada.

