

UNIVERSIDAD PRIVADA DE TACNA INGENIERIA DE SISTEMAS



TITULO:
INFORME DE SESION No 07

CURSO:
BASE DE DATOS II

DOCENTE(ING):
Patrick Cuadros Quiroga

Integrantes:

Roberto Carlos Zegarra Reyes

(2010036175)

Índice

1. Monitorización de base de datos mediante Auditoría	1
1.1. Introducción	1
1.2. Objetivos Generales de la Auditoría de BD	1
1.3. Azure Data Studio	1
2. Desarrollo de Laboratorio	3
2.1. Ejercicio N 01: Utilizando tablas temporales de auditoría	3
2.2. Ejercicio N 02: Utilizando Auditorías	6
2.3. Ejercicio N 03: Utilizando auditorías personalizadas	8
2.4. Ejercicio N 04: Administrando auditorías	10

1. Monitorización de base de datos mediante Auditoría

1.1. Introducción

¿Qué es la Auditoría de BD. Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

- Quién accede a los datos.
- Cuándo se accedió a los datos.
- Desde qué tipo de dispositivo/aplicación.
- Desde qué ubicación en la Red.
- Cuál fue la sentencia SQL ejecutada.
- Cuál fue el efecto del acceso a la base de datos.

Es uno de los procesos fundamentales para apoyar la responsabilidad delegada a IT por la organización frente a las regulaciones y su entorno de negocios o actividad.

1.2. Objetivos Generales de la Auditoría de BD

Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos incluyendo la capacidad de generar alertas con el objetivo de:

- Mitigar los riesgos asociados con el manejo inadecuado de los datos.
- Apoyar el cumplimiento regulatorio.
- Satisfacer los requerimientos de los auditores.
- Evitar acciones criminales.
- Evitar multas por incumplimiento.

La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utiliza esta tecnología.

1.3. Azure Data Studio

Cuando se trabaja con una base de datos o cualquier otro tipo de software, hay momentos en que la experiencia se ve reforzada o dificultada por las herramientas que utiliza para interactuar con ella.

Es por eso por lo que Microsoft presentó Azure Data Studio, un editor de GUI de código abierto que admite Postgres.

The screenshot displays the Microsoft Azure Data Studio interface for a local server connection. The top menu bar includes File, Edit, View, and Help. The left sidebar shows the 'CONNECTIONS' pane with a tree view of 'SERVERS' including 'localhost - <default> (Windows Authentication...)'. The main workspace is titled 'localhost' and shows the 'SERVER DASHBOARD' for the 'Home' instance.

SERVER DASHBOARD

Version	Edition	Computer Name	OS Version
14.0.1000.169	Standard Edition (64-bit)	DESKTOP-GQJLJNH	Windows 10 Education 10.0.19H4 (Build 17134.)

The dashboard includes several panels:

- Tasks:** Contains buttons for 'Restore', 'New Query', 'Learn How To Configure The Dashboard', and 'New Notebook'.
- Search:** A search bar with the text 'Search databases' and a list of databases including master, model, msdb, tempdb, AdventureWorks2014, AdventureWorksLT2012, Cajero, Cajero2, db_electrosur, db_eps, db_proyecto, db_Sistema, db_sistemas, db_Siclientes, db_UPT, OlviZorral, DBOYM, DBVentaLicores2, DWConfiguration, and DWDiagnosics.
- Backup Status:** Shows the last backup time as '13:48:37 7/10/2019' and a summary: '0 Within 24hrs', '2 Older than 24hrs', and '20 No backup found'.
- Database Size (MB):** A horizontal bar chart showing the size of various databases. DWDiagnosics is the largest at approximately 950 MB, followed by AdventureWorks2014 at approximately 250 MB. Other databases like AdventureWorksLT2012, DWConfiguration, DWQueue, db_Sistema, db_UPT, db_sistemas, db_proyecto, and db_electrosur are all very small, near 0 MB.

The bottom status bar shows the connection is to 'localhost - <default>'.

Azure Data Studio está dirigido principalmente a expertos en datos. Por lo tanto, Microsoft también ha desarrollado una extensión de PostgreSQL para Visual Studio Code para aquellos que usan las bases de datos de Postgres como desarrolladores de aplicaciones.

Si su caso de uso principal es la administración de la base de datos, Azure Data Studio puede ser una buena opción.

2

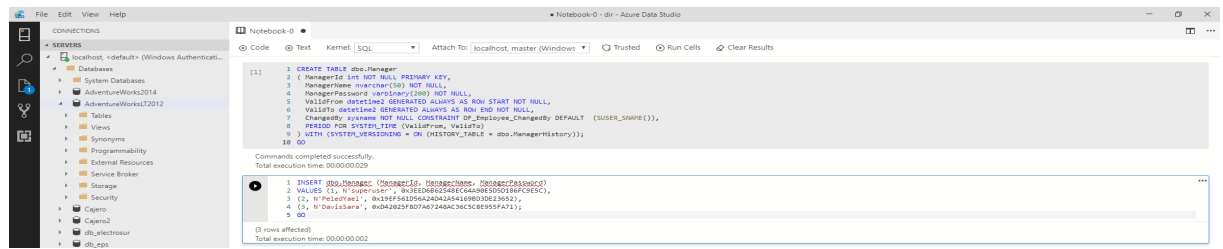
2. Desarrollo de Laboratorio

2.1. Ejercicio N 01: Utilizando tablas temporales de auditoría

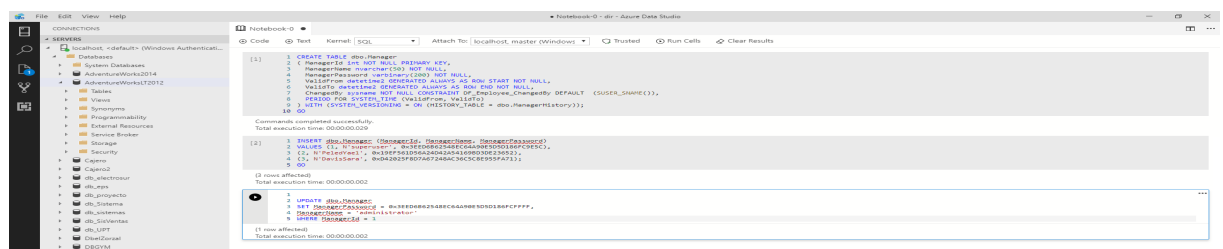
- Paso 1 conecta esta ventana de consulta a tu copia de AdventureWorksLT
- Paso 2 crear una tabla temporal versionada por el sistema



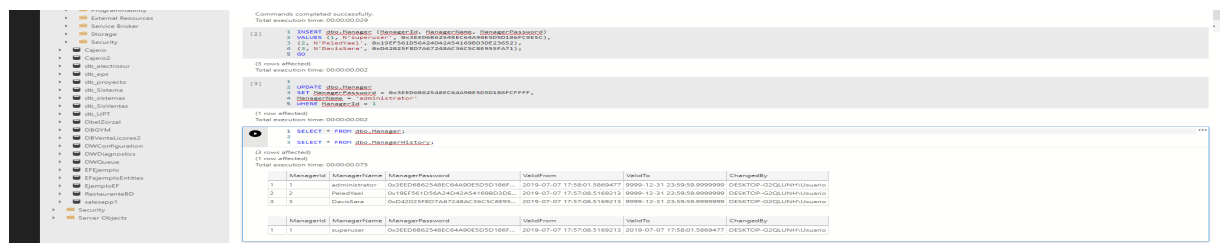
- Paso 3 insertar datos de ejemplo



- Paso 4 actualizar una fila



- Paso 5 examinar tablas de componentes de la tabla temporal



- Paso 6 demuestre POR TODO EL TIEMPO DEL SISTEMA al consultar una tabla temporal TODOS muestra todos los datos en ambas tablas

```

[4] 1 SELECT * FROM dbo.ManagerHistory
2
3 SELECT * FROM dbo.ManagerHistory
4 FOR SYSTEM_TIME ALL
5
(2 rows affected)
(1 row affected)
Total execution time: 00:00:00.075

+-----+
| ManagerId | ManagerName | ManagerPassword | ValidFrom | ValidTo | ChangedBy |
+-----+
| 1 | administrator | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:58:01.5869477 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 2 | PetoelTee | 0x19F561D56A242A54169BD3DE... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 3 | DavidSara | 0x42023F8D7A67248AC36C3CB95... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
+-----+

[5] 1 SELECT * FROM dbo.ManagerHistory
2 FOR SYSTEM_TIME ALL
3
(4 rows affected)
Total execution time: 00:00:00.006

+-----+
| ManagerId | ManagerName | ManagerPassword | ValidFrom | ValidTo | ChangedBy |
+-----+
| 1 | administrator | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:58:01.5869477 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 2 | PetoelTee | 0x19F561D56A242A54169BD3DE... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 3 | DavidSara | 0x42023F8D7A67248AC36C3CB95... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 4 | supervisor | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:57:08.5169213 | 2019-07-07 17:58:01.5869477 | DESKTOP-G2QLNH\Usuario |
+-----+

```

- Paso 7 demuestre POR TIEMPO DE SISTEMA COMO DE cuando se consulta una tabla temporal AS OF muestra un punto en el tiempo.

```

[5] 1 SELECT * FROM dbo.ManagerHistory
2 FOR SYSTEM_TIME ALL
3
(4 rows affected)
Total execution time: 00:00:00.006

+-----+
| ManagerId | ManagerName | ManagerPassword | ValidFrom | ValidTo | ChangedBy |
+-----+
| 1 | administrator | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:58:01.5869477 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 2 | PetoelTee | 0x19F561D56A242A54169BD3DE... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 3 | DavidSara | 0x42023F8D7A67248AC36C3CB95... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 4 | supervisor | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:57:08.5169213 | 2019-07-07 17:58:01.5869477 | DESKTOP-G2QLNH\Usuario |
+-----+

[6] 1 DECLARE @t datetime2 = (SELECT TOP(1) ValidFrom FROM dbo.ManagerHistory WHERE ManagerId = 1)
2 SELECT * FROM dbo.ManagerHistory
3 FOR SYSTEM_TIME AS OF @t
4
(3 rows affected)
Total execution time: 00:00:00.007

+-----+
| ManagerId | ManagerName | ManagerPassword | ValidFrom | ValidTo | ChangedBy |
+-----+
| 1 | administrator | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 2 | PetoelTee | 0x19F561D56A242A54169BD3DE... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 3 | DavidSara | 0x42023F8D7A67248AC36C3CB95... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
+-----+

```

- Paso 8 demostrar que la tabla de historial no se puede editar (ambos comandos generarán un error)

```

[6] 1 DECLARE @t datetime2 = (SELECT TOP(1) ValidFrom FROM dbo.ManagerHistory WHERE ManagerId = 1)
2 SELECT * FROM dbo.ManagerHistory
3 FOR SYSTEM_TIME AS OF @t
4
(3 rows affected)
Total execution time: 00:00:00.007

+-----+
| ManagerId | ManagerName | ManagerPassword | ValidFrom | ValidTo | ChangedBy |
+-----+
| 1 | administrator | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 2 | PetoelTee | 0x19F561D56A242A54169BD3DE... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 3 | DavidSara | 0x42023F8D7A67248AC36C3CB95... | 2019-07-07 17:57:08.5169213 | 9999-12-31 23:59:59.9999999 | DESKTOP-G2QLNH\Usuario |
| 4 | supervisor | 0x3EDD862348EC6A490E5D5D186F... | 2019-07-07 17:57:08.5169213 | 2019-07-07 17:58:01.5869477 | DESKTOP-G2QLNH\Usuario |
+-----+

[7] 1 UPDATE dbo.ManagerHistory SET ChangedBy = 'malicioususer';
2 GO
3 INSERT dbo.ManagerHistory (ManagerId, ManagerName, ManagerPassword)
4 VALUES (99, 'supervisor', 0x3EDD862348EC6A490E5D5D186F09EC)
5 GO
6 GO

Msg 1361, Level 16, State 1, Line 2
Cannot update row in a temporal history table 'master.dbo.ManagerHistory'.
Msg 1361, Level 16, State 1, Line 3
Cannot insert row in a temporal history table 'master.dbo.ManagerHistory'.
Total execution time: 00:00:00.006

```

- Paso 9 demuestre que un usuario con permisos suficientes puede insertar datos engañosos en la columna ChangedBy:

```

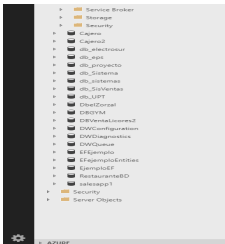
[7] 1 UPDATE dbo.ManagerHistory SET ChangedBy = 'malicioususer';
2 GO
3 INSERT dbo.ManagerHistory (ManagerId, ManagerName, ManagerPassword)
4 VALUES (99, 'supervisor', 0x3EDD862348EC6A490E5D5D186F09EC)
5 GO
6 GO

Msg 1361, Level 16, State 1, Line 2
Cannot update row in a temporal history table 'master.dbo.ManagerHistory'.
Msg 1361, Level 16, State 1, Line 3
Cannot insert row in a temporal history table 'master.dbo.ManagerHistory'.
Total execution time: 00:00:00.006

[8] 1 UPDATE dbo.ManagerHistory
2 SET ManagerId = 99,
3 ManagerName = 'hacked', ChangedBy = 'malicioususer'
4 WHERE ManagerId = 1
5
(1 row affected)
Total execution time: 00:00:00.002

```

- Paso 10 examinar tablas de componentes de la tabla temporal



```

[1] 1 UPDATE dbo.Manager SET ChangedBy = 'maliciousUser';
2 SELECT dbo.ManagerName, ManagerPassword, ManagerPassword
   FROM (SELECT ManagerName, ManagerPassword
         FROM dbo.Manager) AS Manager;
3 GO

Msg 5045, Level 16, State 1, Line 3
Database 'dbo' does not have a tempdb database.
Msg 5045, Level 16, State 1, Line 3
Database 'dbo' does not have a tempdb database.
Total execution time: 00:00:00.000

[2] 1 UPDATE dbo.Manager
   SET ManagerName = 'supervisor',
   ManagerPassword = 'supervisor',
   ValidFrom = '2019-07-07'
2 GO

(1 row affected)
Total execution time: 00:00:00.002

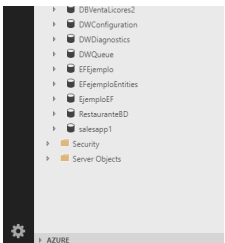
3 SELECT * FROM dbo.Manager;
4 GO

(3 rows affected)
Total execution time: 00:00:00.009

```

ManagerId	ManagerName	ManagerPassword	ValidFrom	ValidTo	ChangedBy
1	hacked	0x0A08	2019-07-07 18:11:05.8272020	9999-12-31 23:59:59.9999999	maliciousUser
2	Pelecfitel	0x196F561D56A24D42A54169BD3DE...	2019-07-07 17:57:08.5168213	9999-12-31 23:59:59.9999999	DESKTOP-GZQLNPHUsuario
3	DavisSara	0x0420C3F8D7A67248AC36C3C8E95...	2019-07-07 17:57:08.5168213	9999-12-31 23:59:59.9999999	DESKTOP-GZQLNPHUsuario

- Paso 11 Cerrar objetos de demostración



```

Total execution time: 00:00:00.009

1 ALTER TABLE dbo.Manager SET (SYSTEM_VERSIONING = OFF);
2 DROP TABLE dbo.Manager;
3 DROP TABLE dbo.ManagerHistory;
4 GO

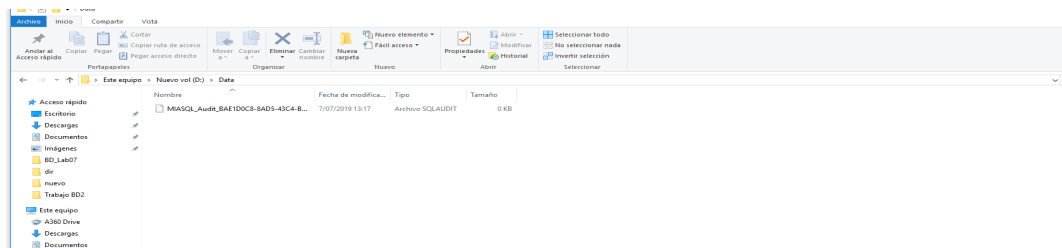
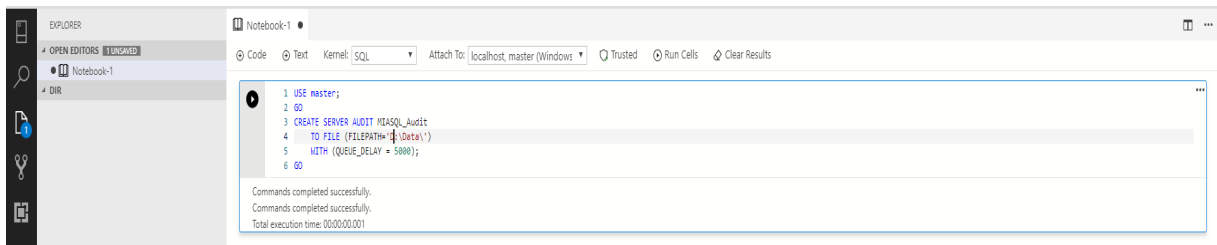
Commands completed successfully.
Total execution time: 00:00:00.005

```

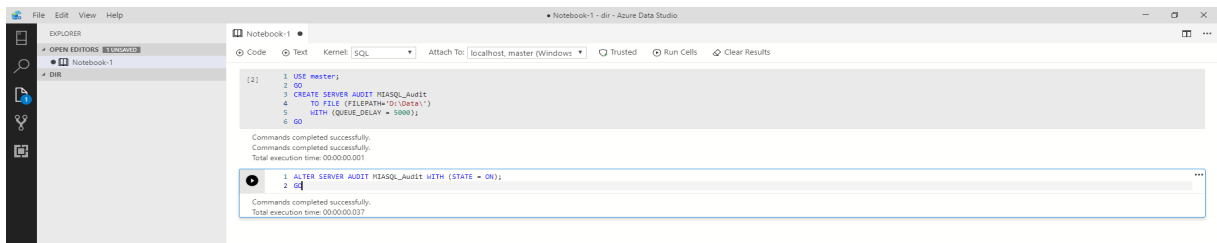
ManagerId	ManagerName	ManagerPassword	ValidFrom	ValidTo	ChangedBy
1	hacked	0x0A08	2019-07-07 18:11:05.8272020	9999-12-31 23:59:59.9999999	maliciousUser
2	Pelecfitel	0x196F561D56A24D42A54169BD3DE...	2019-07-07 17:57:08.5168213	9999-12-31 23:59:59.9999999	DESKTOP-GZQLNPHUsuario
3	DavisSara	0x0420C3F8D7A67248AC36C3C8E95...	2019-07-07 17:57:08.5168213	9999-12-31 23:59:59.9999999	DESKTOP-GZQLNPHUsuario

2.2. Ejercicio N 02: Utilizando Auditorias

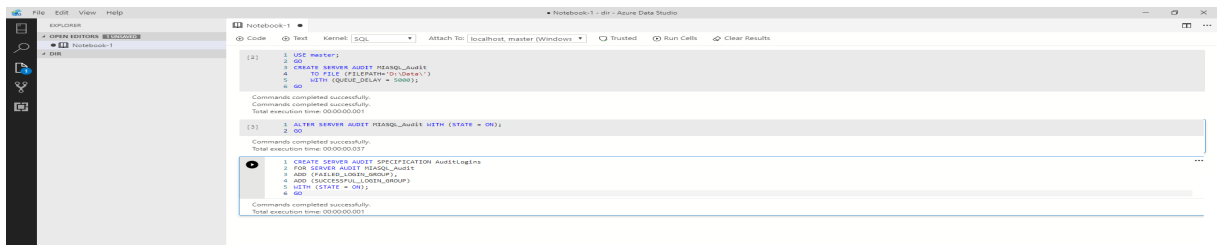
- Paso 1 Crear una auditoria



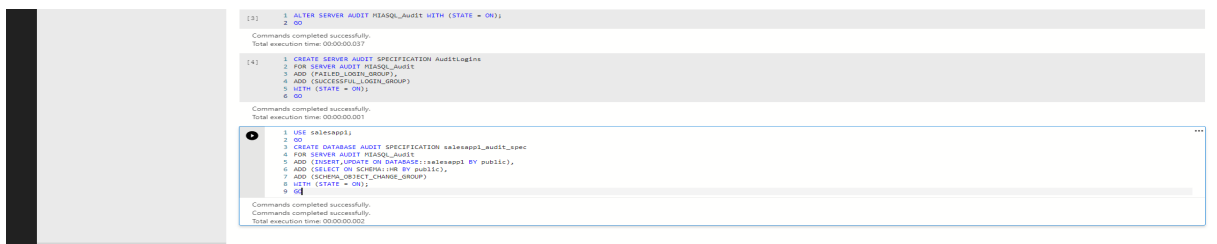
- Paso 2 Habilitar la auditoria



- Paso 3 Crear una especificación de auditoría del servidor



- Paso 4 Crear una especificación de auditoría de base de datos



- Paso 5 Alterar la especificación de auditoría de la base de datos

```

Commands completed successfully.
Total execution time: 00:00:00.001

[5] 1 USE salesrep1;
2 GO
3 CREATE DATABASE AUDIT SPECIFICATION salesrep1_audit_spec
4 FOR SERVER AUDIT MSAQ1_audit WITH (STATE = OFF);
5 ADD (INSERT,UPDATE ON DATABASE::salesrep1 BY public);
6 ADD (SELECT ON SCHEMA::HR BY public);
7 ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP);
8 WITH (STATE = ON);
9 GO

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.002

[6] 1 USE salesrep1;
2 GO
3 ALTER DATABASE AUDIT SPECIFICATION salesrep1_audit_spec WITH (STATE = OFF);
4 GO
5 ALTER DATABASE AUDIT SPECIFICATION salesrep1_audit_spec
6 ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP);
7 WITH (STATE = ON);
8 GO

Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.001

```

- Paso 6 Examinar metadatos de auditoría

```

[6] 1 USE salesrep1;
2 GO
3 ALTER DATABASE AUDIT SPECIFICATION salesrep1_audit_spec WITH (STATE = OFF);
4 GO
5 ALTER DATABASE AUDIT SPECIFICATION salesrep1_audit_spec
6 ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP);
7 WITH (STATE = ON);
8 GO

Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.001

[7] 1
2 SELECT * FROM sys.server_audits;

(1 row affected)
Total execution time: 00:00:00.019

audit_id | name | audit_guid | create_date | modify_date | principal_id | type | type_desc | on_failure | on_failure_desc | is_state_enabled | queue_delay | predicate
1 | 65537 | MIAQ1_Audit | bae1d0b-8ae5-43d4-b78e-5669217... | 2019-07-07 13:16:40.737 | 2019-07-07 13:16:40.737 | 1 | FL | FILE | 0 | CONTINUE | 1 | 5000 | NULL

```

- Paso 7 Examinar los metadatos de especificación de auditoría del servidor

```

[7] 1 SELECT * FROM sys.server_audits;

(1 row affected)
Total execution time: 00:00:00.019

audit_id | name | audit_guid | create_date | modify_date | principal_id | type | type_desc | on_failure | on_failure_desc | is_state_enabled | queue_delay | predicate
1 | 65537 | MIAQ1_Audit | bae1d0b-8ae5-43d4-b78e-5669217... | 2019-07-07 13:16:40.737 | 2019-07-07 13:16:40.737 | 1 | FL | FILE | 0 | CONTINUE | 1 | 5000 | NULL

[8] 1 SELECT * FROM sys.server_audit_specifications;
2 SELECT *
3 FROM sys.server_audit_specification_details AS sd
4 JOIN sys.dm_audit_actions AS aa
5 ON aa.name = sd.audit_action_name COLLATE Latin1_General_CI_AS_KS_WS;

(1 row affected)
(2 rows affected)
Total execution time: 00:00:00.031

server_specification_id | name | create_date | modify_date | audit_guid | is_state_enabled
1 | 65536 | AuditLogins | 2019-07-07 13:18:05.450 | 2019-07-07 13:18:05.450 | bae1d0b-8ae5-43d4-b78e-5669217... | 1

server_specification_id | audit_action_id | audit_action_name | class | class_desc | major_id | minor_id | audited_principal_id | audited_result | is_group | action_id | name | class_desc | covering_action_name | parent_class_id
1 | 65536 | LOP1 | FAILED_LOGIN_GROUP | 100 | SERVER | 0 | 0 | 2 | SUCCESS AND FAILURE | 1 | LOP1 | FAILED_LOGIN_GROUP | SERVER | NULL | NULL
2 | 65536 | L00D | SUCCESSFUL_LOGIN_GROUP | 100 | SERVER | 0 | 0 | 2 | SUCCESS AND FAILURE | 1 | L00D | SUCCESSFUL_LOGIN_GROUP | SERVER | NULL | NULL

```

- Paso 8 Examinar los metadatos de especificación de auditoría de base de datos

```

[8] 1 SELECT * FROM sys.database_audit_specifications;
2 SELECT *
3 FROM sys.database_audit_specification_details AS sd
4 JOIN sys.dm_audit_actions AS aa
5 ON aa.name = sd.audit_action_name COLLATE Latin1_General_CI_AS_KS_WS
6 AND aa.class_desc = sd.class_desc COLLATE Latin1_General_CI_AS_KS_WS;

(1 row affected)
(5 rows affected)
Total execution time: 00:00:00.031

database_specification_id | name | create_date | modify_date | audit_guid | is_state_enabled
1 | 65536 | salesrep1_audit_spec | 2019-07-07 13:18:32.347 | 2019-07-07 13:18:32.347 | bae1d0b-8ae5-43d4-b78e-5669217... | 1

database_specification_id | audit_action_id | audit_action_name | class | class_desc | major_id | minor_id | audited_principal_id | audited_result | is_group | action_id | name | class_desc | covering_action_name | parent_class_id
1 | 65536 | GRO | SCHEMA_OBJECT_PERMISSION_CHANGE | 0 | DATABASE | 0 | 0 | 0 | SUCCESS AND FAILURE | 1 | GRO | SCHEMA_OBJECT_PERMISSION_CHANGE | DATABASE | NULL | NULL
2 | 65536 | IN | INSERT | 0 | DATABASE | 0 | 0 | 0 | SUCCESS AND FAILURE | 1 | IN | INSERT | DATABASE | SCHEMA_OBJECT_PERMISSION_CHANGE | NULL
3 | 65536 | MHO | SCHEMA_OBJECT_CHANGE_GROUP | 0 | DATABASE | 0 | 0 | 0 | SUCCESS AND FAILURE | 1 | MHO | SCHEMA_OBJECT_CHANGE_GROUP | DATABASE | NULL | NULL
4 | 65536 | UP | UPDATE | 0 | DATABASE | 0 | 0 | 0 | SUCCESS AND FAILURE | 1 | UP | UPDATE | DATABASE | SCHEMA_OBJECT_CHANGE_GROUP | NULL
5 | 65536 | SL | SELECT | 3 | SCHEMA | 5 | 0 | 0 | SUCCESS AND FAILURE | 0 | SL | SELECT | SCHEMA | NULL | NULL

```

- Paso 9 quitar la auditoria

```

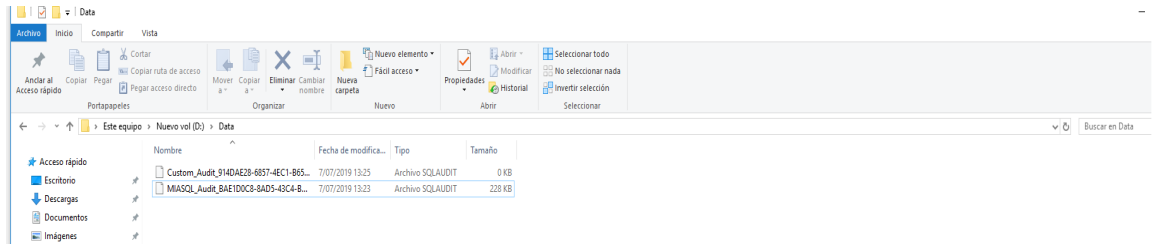
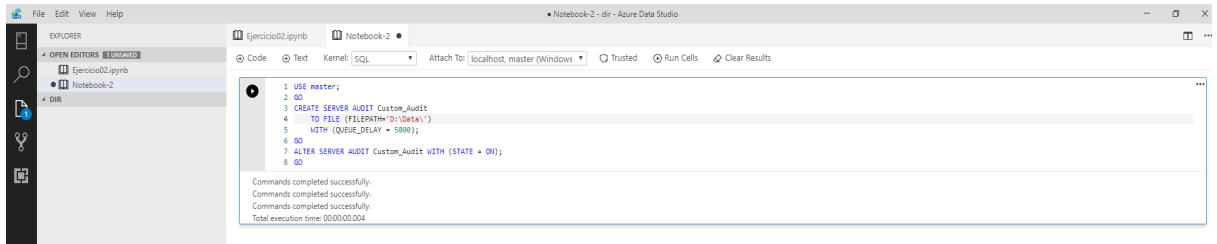
[9] 1 USE master;
2 GO
3 ALTER SERVER AUDIT MSAQ1_audit WITH (STATE = OFF);
4 DROP SERVER AUDIT MSAQ1_audit;
5 GO
6
7 ALTER SERVER AUDIT SPECIFICATION AuditLogins WITH (STATE = OFF);
8 DROP SERVER AUDIT SPECIFICATION AuditLogins;
9 GO
10
11 USE salesrep1;
12 GO
13 ALTER DATABASE AUDIT SPECIFICATION salesrep1_audit_spec WITH (STATE = OFF);
14 DROP DATABASE AUDIT SPECIFICATION salesrep1_audit_spec;
15 GO

Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.071

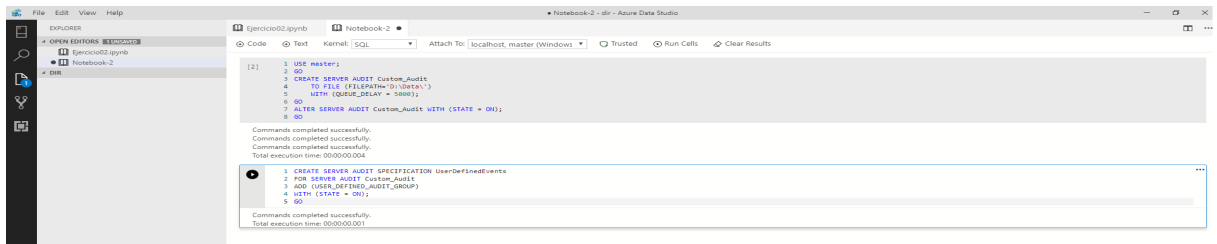
```

2.3. Ejercicio N 03: Utilizando auditorías personalizadas

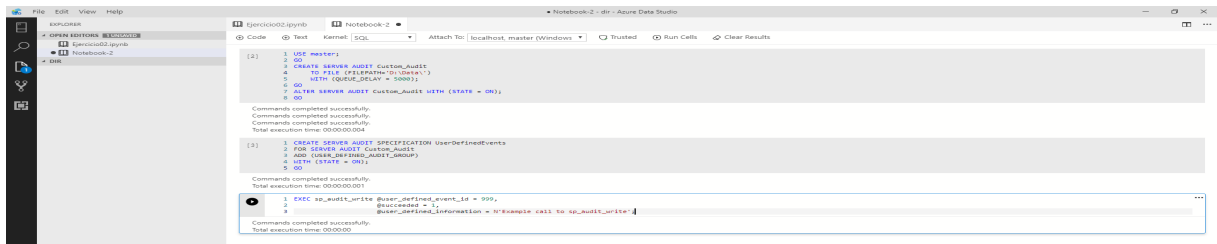
- Paso 1 Crear una auditoria



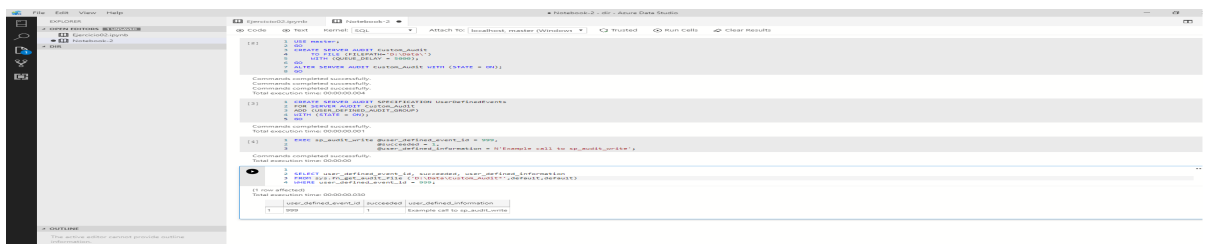
- Paso 2 crear una especificación de auditoría del servidor que incluya el grupo de acción USER_DEFINED_AUDIT_GROUP



- Paso 3 llama a sp_audit write directamente



- Paso 4 Demostrar cómo aparece un evento personalizado en la auditoría.



- Paso 5 demostrar el uso de sp audit write en un procedimiento almacenado

```

1 USE salesaword;
2 GO
3 CREATE PROCEDURE sp_audit_write
4     @orderid INT,
5     @productid INT,
6     @discount NUMERIC(4,2)
7 AS
8 SET NOCOUNT ON;
9
10 DECLARE @msg VARCHAR(4000);
11
12 SET @msg = 'OrderID = ' + CAST(@orderid AS VARCHAR(10)) + ', ProductID = ' + CAST(@productid AS VARCHAR(10)) + ', Discount = ' + CAST(@discount AS VARCHAR(10));
13
14 EXEC sp_audit_write @user_defined_event_id = 999,
15     @succeeded = 1,
16     @user_defined_information = @msg;
17
18 END
19
20 UPDATE Sales.OrderDetails
21 SET discount = @discount
22 WHERE orderid = @orderid
23 AND productid = @productid
24
25 GO

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.003

user_defined_event_id	succeeded	user_defined_information
999	1	Example call to sp_audit_write

- Paso 6 llame al procedimiento almacenado dos veces La primera llamada no debe generar un evento de auditoría personalizado La segunda llamada debe generar un evento de auditoría personalizado

```

18 EXEC sp_audit_write @user_defined_event_id = 999,
19     @succeeded = 1,
20     @user_defined_information = @msg;
21
22 END
23
24 UPDATE Sales.OrderDetails
25 SET discount = @discount
26 WHERE orderid = @orderid
27 AND productid = @productid
28
29 GO

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.003

```

1 EXEC @? sp_audit_write @orderid = 10249, @productid = 11, @discount = 0.05
2 EXEC @? sp_audit_write @orderid = 10249, @productid = 42, @discount = 0.45

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.395

- Paso 7 examinar los datos de auditoría

```

27 GO

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.003

```

1 EXEC @? sp_audit_write @orderid = 10249, @productid = 11, @discount = 0.05
2 EXEC @? sp_audit_write @orderid = 10249, @productid = 42, @discount = 0.45

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.395

```

1 SELECT user_defined_event_id, succeeded, user_defined_information
2 FROM sys.fn_get_audit_file ('\\data\Custom_Audit', default, default)
3 WHERE user_defined_event_id = 999;

```

(1 row affected)
Total execution time: 00:00:00.030

user_defined_event_id	succeeded	user_defined_information
998	1	Order=10248/Product=42/discount=0.450

- Paso 8 abandonar la auditoria

```

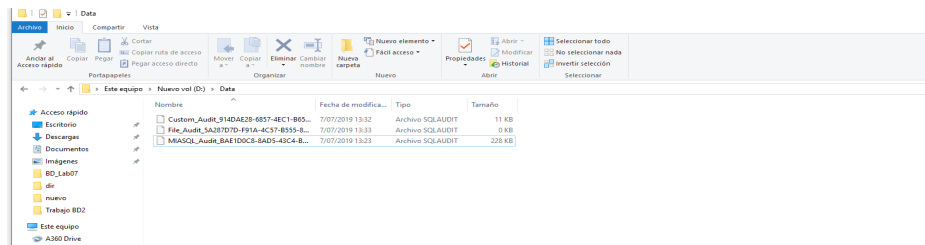
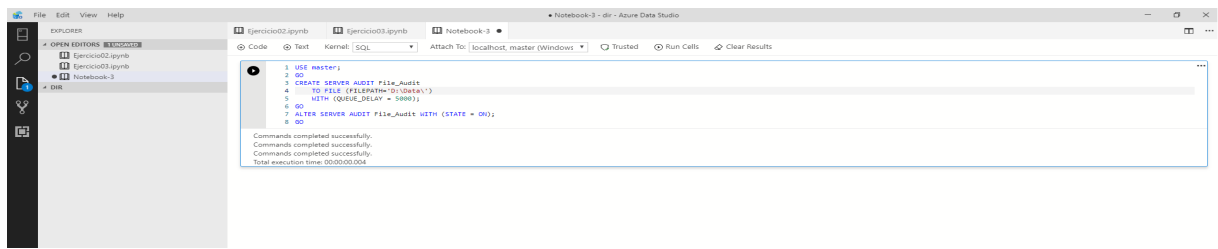
1 USE master;
2 GO
3 ALTER SERVER AUDIT Custom_Audit WITH (STATE = OFF);
4 DROP SERVER AUDIT Custom_Audit;
5 GO
6
7 ALTER SERVER AUDIT SPECIFICATION UserDefinedEvents WITH (STATE = OFF);
8 DROP SERVER AUDIT SPECIFICATION UserDefinedEvents;
9 GO

```

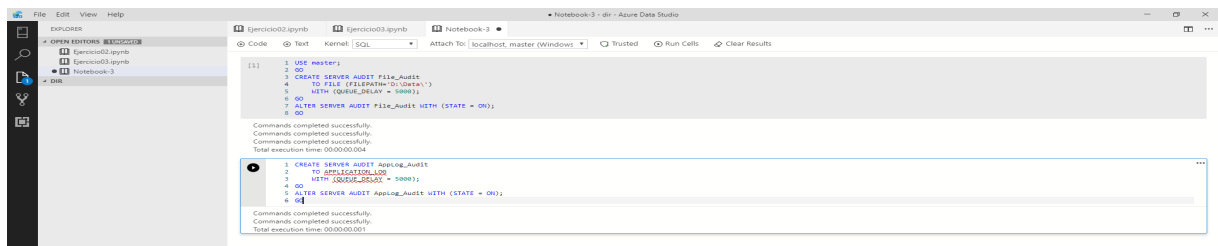
Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.007

2.4. Ejercicio N 04: Administrando auditorías

- Paso 1 crear una auditoría con un archivo de destino



- Paso 2 crear una auditoría con un destino de registro de aplicación de Windows



- Paso 3 agregar la misma especificación de auditoría de base de datos a ambas auditorías



- Paso 4 Ejecutar una instrucción de selección simple que coincida con la especificación de auditoría

```

1 FOR SERVER AUDIT Applog_Audit;
2 GO
3 ADD SELECT ON SCHEMA::Sales BY pub151c;
4 WITH (STATE = ON);
5 GO

```

Commands completed successfully.
Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.001

```

1 SELECT TOP 10 * FROM Sales.Customer;
2 GO

```

(10 rows affected)
Total execution time: 00:00:00.006

customerid	companyname	contactname	contacttitle	address	city	region	postalcode	country	phone	fax
1	Customer HR28B	Allen, Michael	Sales Representative	Ottawa Str. 0123	Berlin	NULL	10092	Germany	030-3456789	030-0123456
2	Customer MLTON	Passek, Mark	Owner	Avenida de la Constitución 3478	México D.F.	NULL	10077	Mexico	(5) 789-0123	(5) 456-7890
3	Customer KBLUG	Pesquet, John	Owner	Manhattan 7890	México D.F.	NULL	10097	Mexico	(5) 123-4567	NULL
4	Customer HFR22	Arnold, Tomten	Sales Representative	7690 Hansover Sq.	London	NULL	10046	UK	(171) 456-7890	(171) 456-7891
5	Customer HNYL2	Piggott-Smith, Tom	Order Administrator	Bergengraben 1078	Ludwig	NULL	10112	Sweden	(0821) 45 67 89	(0821) 23 45 67
6	Customer XH4VF	Poland, Carole	Sales Representative	Forsterstr. 7890	Mannheim	NULL	10117	Germany	0621-67890	0621-12345
7	Customer QGVLA	Bansal, Dushyant	Marketing Manager	2345 place Kieber	Strasbourg	NULL	10089	France	67.89.01.23	67.89.01.24
8	Customer QHWH	Hjima, Julia	Owner	C/ Araquil 0123	Madrid	NULL	10104	Spain	(91) 345 67 89	(91) 012 34 56
9	Customer RTXGC	Raghu, Amrithash	Owner	6789 rue des Bouchers	Marseille	NULL	10105	France	23.45.67.89	23.45.67.80
10	Customer EEAUV	Bassoli, Pilar Colome	Accounting Manager	8901 Tasavassen Blvd.	Tasavassen	BC	10111	Canada	(804) 901-2345	(804) 678-9012

- Paso 5 Examine la salida de auditoría basada en archivos. Demostrar algunos de los campos más útiles.

```

1 SELECT *
2 FROM sys.fn_get_audit_file ('D:\Data\File_Audit', default, default);

```

(2 rows affected)
Total execution time: 00:00:00.016

event_time	sequence_number	action_id	succeeded	permission_bitmask	is_column_permission	session_id	server_principal_id	database_principal_id	target_server_principal_id	target_database_principal_id	object_id	class
2019-07-07 18:33:37.8648164	1	AUSC	1	0x00000000000000000000000000000000...	0	149	259	0	0	0	0	A
2019-07-07 18:36:06.7199218	1	SL	1	0x00000000000000000000000000000000...	1	149	259	1	0	0	485576768	U

- Paso 6 examinar la salida de auditoría de registro de aplicación de Windows. Usar el visor de eventos
- Paso 7 abandone las auditorías y las especificaciones de auditoría, tenga en cuenta que las auditorías y las especificaciones deben desactivarse antes de poder retirarse

```

1 ALTER DATABASE AUDIT SPECIFICATION sales_select_spec_aplog WITH (STATE = OFF);
2 DROP DATABASE AUDIT SPECIFICATION sales_select_spec_aplog;
3 ALTER DATABASE AUDIT SPECIFICATION sales_select_spec_file WITH (STATE = OFF);
4 DROP DATABASE AUDIT SPECIFICATION sales_select_spec_file;
5 GO
6 USE master;
7 ALTER SERVER AUDIT Applog_Audit WITH (STATE = OFF);
8 DROP SERVER AUDIT Applog_Audit;
9 ALTER SERVER AUDIT File_Audit WITH (STATE = OFF);
10 DROP SERVER AUDIT File_Audit;
11 GO

```

Commands completed successfully.
Commands completed successfully.
Total execution time: 00:00:00.044

event_time	sequence_number	action_id	succeeded	permission_bitmask	is_column_permission	session_id	server_principal_id	database_principal_id	target_server_principal_id	target_database_principal_id	object_id	class
2019-07-07 18:33:37.8648164	1	AUSC	1	0x00000000000000000000000000000000...	0	149	259	0	0	0	0	A
2019-07-07 18:36:06.7199218	1	SL	1	0x00000000000000000000000000000000...	1	149	259	1	0	0	485576768	U