



ribadeo



**Análisis de Permisos Efectivos de una
Aplicación en SQL Server**

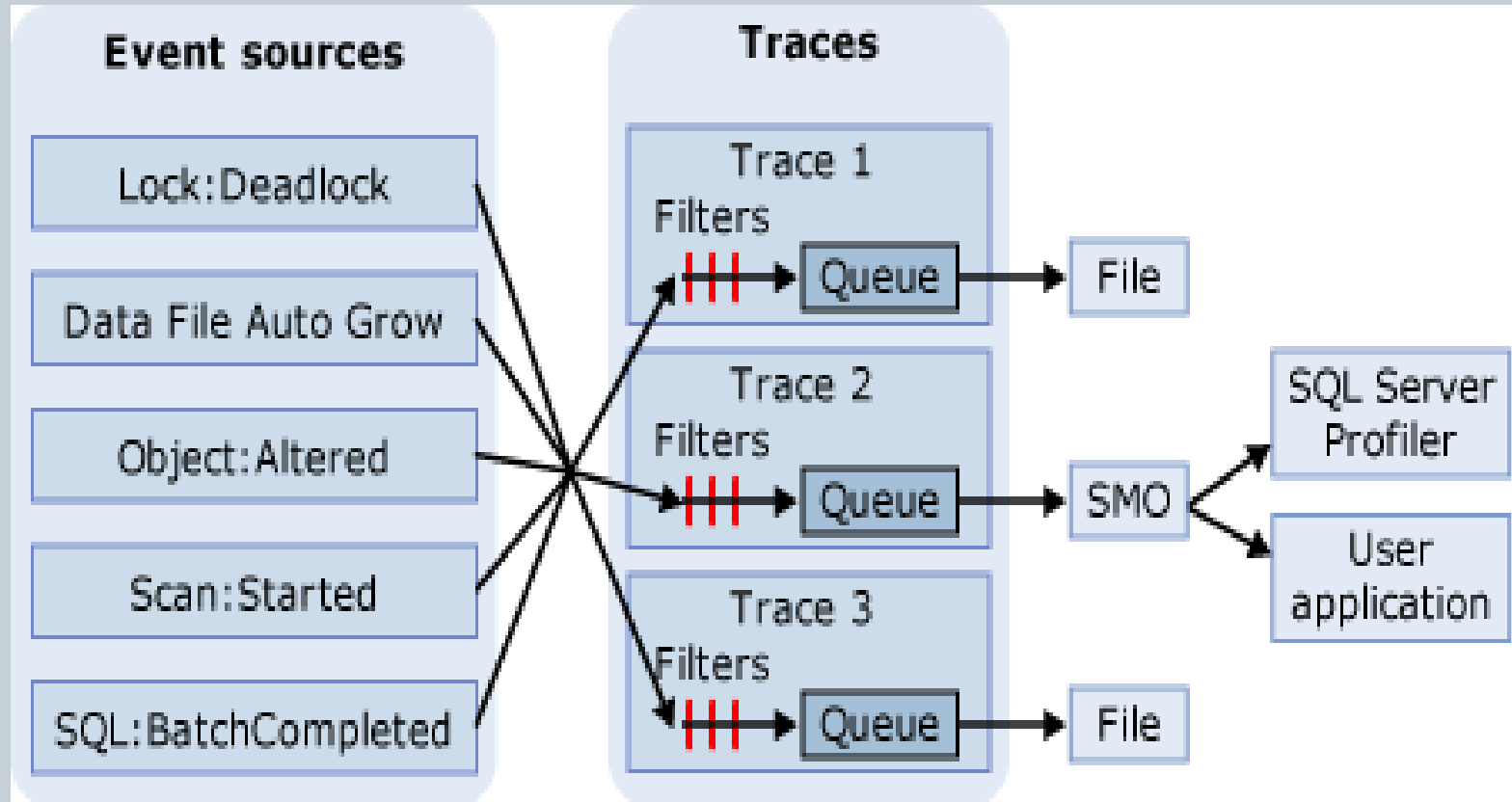
Trazas

2

- Son los objetos que se usan en SQL Server para recolectar y analizar los eventos que se generan en una instancia.
- Un evento en cualquier acción que se ejecute dentro de la instancia. Existen múltiples tipos de eventos que permiten analizar información de casi cualquier acción de la instancia.

Arquitectura de Trazas

3



Proceso de Creación de una Traza

4

Creación del Objeto Traza

Seteo de Eventos a recolectar

Seteo de Filtros sobre columnas

Cambio de Estado de la Traza a Activo

Creación del Objeto Traza

5

- **SP_TRACE_CREATE:** Crea una definición de traza. La nueva traza estará en estado de detención

```
sp_trace_create [ @traceid = ] trace_id OUTPUT ,  
  [ @options = ] option_value ,  
  [ @tracefile = ] 'trace_file' [ ,  
  [ @maxfilesize = ] max_file_size ]  
  [ , [ @stoptime = ] 'stop_time' ]  
  [ , [ @filecount = ] 'max_rollover_files' ]
```

- <http://msdn.microsoft.com/es-es/library/ms190362.aspx>

Seteo de los Eventos a Recolectar

6

- **SP_TRACE_SETEVENT**: Agrega o quita un evento o una columna de evento de una traza. **sp_trace_setevent** sólo puede ejecutarse en trazas existentes que estén detenidas

```
sp_trace_setevent [ @traceid = ] trace_id  
    , [ @eventid = ] event_id  
    , [ @columnid = ] column_id  
    , [ @on = ] on
```

- <http://msdn.microsoft.com/es-es/library/ms186265.aspx>

Seteo de Filtros sobre Columnas

7

- **SP_TRACE_SETFILTER**: Aplica un filtro a una traza. **sp_trace_setfilter** sólo se puede ejecutar en trazas existentes que estén detenidas

```
sp_trace_setfilter [ @traceid = ] trace_id  
    , [ @columnid = ] column_id  
    , [ @logical_operator = ] logical_operator  
    , [ @comparison_operator = ] comparison_operator  
    , [ @value = ] value
```

- <http://msdn.microsoft.com/es-es/library/ms174404.aspx>

- **SP_TRACE_SETSTATUS:** Modifica el estado actual de la traza especificada

```
sp_trace_setstatus [ @traceid = ] trace_id ,  
    [ @status = ] status
```

Estado	Descripción
0	Detiene la traza especificada.
1	Inicia la traza especificada.
2	Cierra la traza especificada y elimina su definición del servidor.

- <http://msdn.microsoft.com/es-es/library/ms176034.aspx>

Proceso de Lectura de una Traza

9

Detención y Cierre
de la Traza

Lectura del Archivo
de Traza

Detención y Cierre de la Traza

10

- Se ejecuta la llamada al stored procedure `sp_trace_setstatus` dos veces consecutivas con los parametros de estado “0” y “2” para la traza especificada.
 - `Sp_trace_setstatus @traceID, 0`
 - `Sp_trace_setstatus @traceID, 2`

Lectura del Archivo de Traza

11

- **FN_TRACE_GETTABLE**: Devuelve el contenido de uno o varios archivos de traza en formato tabular

`fn_trace_gettable (filename , number_files)`

- Se ejecuta un query sobre el resultado de la función
 - `SELECT * INTO temp_trc FROM fn_trace_gettable('c:\temp\my_trace.trc', default)`
- <http://msdn.microsoft.com/es-es/library/ms188425.aspx>

Demo

12

The screenshot shows a window titled "SQL Server Effective Permissions" with a blue title bar and standard Windows window controls (minimize, maximize, close). The window contains a menu bar with "Exit" and "Help". Below the menu bar are several input fields:

- Host: habbamonte
- Port: 1433
- User: sa
- Password: •••••
- Path: C:\trazas
- Database: hernan

Below these fields is a large, empty grey rectangular area. At the bottom of the window, there is a button labeled "Start collecting" and a status bar that reads "Disconnected".

1

- Creación de Stored Procedures en MASTER

2

- Configuración de parámetros de conexión e inicio de la recolección

3

- Detención de la recolección y generación del reporte

Demo: Creación de SP

14

The screenshot displays the Microsoft SQL Server Management Studio interface. The 'Object Explorer' on the left shows the server hierarchy for 'SQL Server 10.0.1600 - sa'. The 'Query Editor' window is open to a query named 'Seg50yApp_Dat...ter (sa (54))' in the 'master' database. The query contains the following T-SQL code:

```
CREATE PROCEDURE Seg50yApp_DataCollect @TracePath varchar(1024), @DatabaseName nvarchar(256) AS
BEGIN

    DECLARE @TraceName NVARCHAR(1100)
    DECLARE @TraceID INT
    DECLARE @TrcAux INT
    DECLARE @FileSize BIGINT
    DECLARE @On BIT
    DECLARE @DirectoryCreateCmd varchar(1100)
    DECLARE @TraceDeleteCmd varchar(1100)

    IF SUBSTRING(@TracePath, LEN(@TracePath), 1) <> '\\'
        SET @TracePath = @TracePath + '\\'

    SET @TraceName = @TracePath + @DatabaseName + '_SegSO_EffPerm'

    SET @DirectoryCreateCmd = 'mkdir ' + @TracePath
    EXEC master..XP_CMDSHELL @DirectoryCreateCmd, no_output

    SET @TrcAux = (SELECT traceid FROM fn_trace_getinfo(0) WHERE property = 2 and CONVERT(nvarchar(256),value) = @TraceName)
    IF @TrcAux IS NOT NULL
    BEGIN
        EXEC master..SP_TRACE_SETSTATUS @TrcAux,0 --Se detiene la recoleccion de la traza
        EXEC master..SP_TRACE_SETSTATUS @TrcAux,2 --Se elimina la traza
    END

    SET @TraceDeleteCmd = 'del ' + @TracePath + @DatabaseName + '_SegSO_EffPerm*.trc'
    EXEC master..XP_CMDSHELL @TraceDeleteCmd, no_output

    SET @FileSize = 50
    SET @On = 1
    EXEC master..SP_TRACE_CREATE @TraceID output,
        @options = 2,
        @tracefile = @TraceName,
```

The status bar at the bottom indicates the connection is to '(local) (10.0 RTM) sa (54) master' with 0 rows affected.

Demo: Configuración de Parámetros e Inicio de Recolección

15

SQL Server Effective Permissions

Exit Help

Host: habbamonte

Port: 1433

User: sa

Password: ●●●●

Path: C:\trazas

Database: heman

Start collecting

Disconnected

Demo: Detención de la Recolección y Generación del Reporte

16

SQL Server Effective Permissions

Exit Help

Host: habbamonte
 Port: 1433
 User: sa
 Password: ●●●●
 Path: C:\vrazas
 Database: hernan

Exclid	DatabaseName	TimeStamp	OperationClass	ApplicationName	LoginName	ObjectName	ObjectType	OperationType	Success
▶ 1	hernan	27/10/2009 10:07	Data Definition L...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	ALTER	1
1	hernan	27/10/2009 10:07	Data Definition L...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	CREATE	1
1	hernan	27/10/2009 10:07	Data Definition L...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	DROP	1
1	hernan	27/10/2009 10:07	Data Manipulatio...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	DELETE	1
1	hernan	27/10/2009 10:07	Data Manipulatio...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	INSERT	1
1	hernan	27/10/2009 10:07	Data Manipulatio...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	SELECT	1
1	hernan	27/10/2009 10:07	Data Manipulatio...	Microsoft SQL Se...	sa	hernan1234	(User-defined) Ta...	UPDATE	1
1	hernan	28/10/2009 18:41	Data Definition L...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	ALTER	1
1	hernan	28/10/2009 18:41	Data Definition L...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	CREATE	1
1	hernan	28/10/2009 18:41	Data Definition L...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	DROP	1
1	hernan	28/10/2009 18:41	Data Manipulatio...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	DELETE	1
1	hernan	28/10/2009 18:41	Data Manipulatio...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	INSERT	1
1	hernan	28/10/2009 18:41	Data Manipulatio...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	SELECT	1
1	hernan	28/10/2009 18:41	Data Manipulatio...	Microsoft SQL Se...	sa	test123456	(User-defined) Ta...	UPDATE	1
1	hernan	28/10/2009 18:41	Data Manipulatio...	Microsoft SQL Se...	sa	system_objects\$	View	SELECT	1
*									

Start collecting

Disconnected

Preguntas

17

