Using SQL Server Extended Events

IDERA SQL Compliance Manager 5.4 and later allows you to take advantage of the SQL Server Extended Events (XEvents) feature to track and archive specific events occurring in your monitored environment. SQL Server Extended Events is an event handling system that offers lower overhead and delivers performance gains over the default SQL trace method. In SQL Compliance Manager 5.4 and later, only SELECT and DML events for SQL Server 2012 and later versions are supported by this feature. All functionality that works on top of these events, such as DML /Select filtering, Before-After data, sensitive column auditing, and more, work with this new method of capturing event data.

When Extended Events mode is enabled, events generate XEL files instead of trace files (.xel rather than .trc) but the files still are located in the Agent trace directory.

There are two ways to enable Extended Event capture:

- Through stored procedures.
- Through the Registered SQL Server Properties window - Audited Activities tab in the Windows Management Console.

Extended Events captures extra Execute events

Due to differences in how Microsoft has implemented Extended Events compared to other auditing methods, when auditing via Extended Events the user will see extra Execute events as compared to the same data captured by other auditing methods.

Extended Events does not Support Auditing a specific table/object

Due to technical limitations, Extended Events does not support auditing for a specific table/object. To audit a specific table /object please audit using SQL Trace or SQL Server Audit Logs.

Prerequisites and conditions for enabling auditing using Extended Events

IDERA SQL Compliance Manager supports Extended Events based auditing for SQL Server 2012 or above. The following prerequisites and conditions are required to switch auditing based on Extended Events.

- During installation
  - SQL Compliance Manager checks to make sure that Microsoft.SqlServer.XEvent.Linq.dll is available. If not, installation aborts.
- While enabling Extended Events from the web console
  - SQL Compliance Manager checks for the following conditions, which all must be met to successfully enable Extended Events:
    - Agent is reachable
    - SQL Server 2012 or above
    - SQL Compliance Manager Agent 5.4 or above
    - Microsoft.SqlServer.XEvent.Linq.dll is available (along with Microsoft.SqlServer.XE.Core.dll if Linq.dll is obtained from SQL Server SMO 2014 or 2016)

    Note that these conditions must be checked and confirmed manually if Extended Events is being enabled using a SQL stored procedure.

Enable Extended Event mode using stored procedures

To enable Extended Event mode using stored procedures, go to the location where the IDERA SQL Compliance Manager Console application is installed, and then execute the stored procedure `[dbo].[sp_enable_ExtendedEvents]`. For example:

```
EXEC [dbo].[sp_enable_ExtendedEvents] <SERVER_NAME>,<YES/NO>
```

Enable Extended Event mode using the Windows Management Console

Users wanting to take advantage of SQL Server Extended Events auditing capabilities can do so by completing the following steps:

1. Right-click the instance you want to audit and select **Properties**.
2. In the **Registered SQL Server Properties** window, select the **Audited Activities** tab.
3. Under the **Capture DML and Select activities** options, select the **Via Extended Events** option.
4. Click **OK**.

For more information about enabling this feature using the Windows Management Console, see Registered SQL Server Properties window - Audited Activities tab.