SQL Server events you can audit

IDERA SQL Compliance Manager allows you to audit specific types of SQL Server event data, and distinguish between successful operations and failed operations. Whether an operation succeeds or fails is dependent upon whether the login permissions are correct.

Data types and corresponding events

SQL Compliance Manager captures the following types of event data.

Data Type	Events Audited	Description
Logins	• Successful logins • Logouts • Failed logins Impersonation	Audits login activity if an access check is performed and the event status is recorded (success or failure) at the server level
Administration	• Backups Restores • DBCC • Change server settings • Alter trace Database operation	Audits common administrative tasks on the SQL Server instance
Security	• Add login • Add role • Grant, Revoke, Deny • Change role password • Change login properties • Change owner	Audits all SQL security model activity

Database Definition (DDL)	• Derived permission • SQL statement permission • Database access	Audits create, drop, and alter operations performed on SQL Server objects, database objects, and schema object
DML	Object permissions	Audits common database operations, such as: • UPDATE • INSERT • DELETE
Select	SELECT	Audits all SELECT statements executed on database table
Privileged User	All	Audits all privileged user activity at any level ***If the privileged user is also a trusted user*** , SQL Compliance Manager continues to audit this user because of its elevated privileges. For example, a service account that is a member of the sysadmin fixed SQL Server role will continue to be audited even though the account is designated as trusted.
User defined	All	Audits all custom events generated using the `sp_trace_generateevent` stored procedure

Data levels

You can capture different event data at one or more of the following levels:

- SQL Server instance
- Database
- Database object, such as a table

This flexibility allows you to achieve precise and granular compliance. For example, you can configure different audit settings for multiple databases hosted on a single registered SQL Server instance.