Server-level audit settings

You can specify which SQL events you want to audit at the server level. IDERA SQL Compliance Manager applies these settings to the registered SQL Server instance. These settings are not applied to the hosted databases.

You can configure server audit settings when you register a new SQL Server instance or later as your auditing needs change. For more information about individual SQL events, see Microsoft SQL Server Books Online.

Event class	SQL Server version	Description
Audit Add Login	SQL Server 2000 only	Records when a SQL Server login is added to or dropped from a registered SQL Server instance In SQL Server 2005 and later, this event class is Audit Server Principal Management
Audit Add Login To Server Role	SQL Server 2000 and later	Records when a login is added to or removed from a server role
Audit Change Database Owner	SQL Server 2005 and later	Records when the ALTER AUTHORIZATION statement is used to specify a different database owner
Audit Database Management	SQL Server 2005	Records all DROP, ALTER, and CREATE operations on a database
Audit Login	SQL Server 2000 and later	Records all successful logins on the registered SQL Server instance
Audit Login Change Password	SQL Server 2000 and later	Records all password changes for logins on the registered SQL Server instance
Audit Login Change Properties	SQL Server 2000 and later	Records changes in default database and language properties for all logins on the registered SQL Server instance
Audit Login Failed	SQL Server 2000 and later	Records all logins that failed an access check on the registered SQL Server instance
Audit Login GDR	SQL Server 2000 only	Records all GRANT, REVOKE, or DENY actions on Windows 2000 user account login rights In SQL Server 2005 and later, this event class is Audit Server Principal Management
Audit Object Derived Permission	SQL Server 2000 only	Records CREATE and DROP commands executed on a server object, such as CREATE DATABASE or DROP DATABASE In SQL Server 2005 and later, this event class is Audit Database Management
Audit Server Alter Trace	SQL Server 2005 and later	Records when an ALTER TRACE permission check is executed for a T-SQL statement that creates, configures, or filters a SQL trace
Audit Server Object GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements on the audited schema object, such as a table or function
Audit Server Object Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on server objects
Audit Server Object Take Ownership	SQL Server 2005 and later	Records when ownership of an audited server object changes
Audit Server Operation	SQL Server 2005 and later	Records all security operations executed on the audited server
Audit Server Principal Impersonation	SQL Server 2005 and later	Records when impersonation is used to access or act on a server object
Audit Server Principal Management	SQL Server 2005 and later	Records all DROP, ALTER, and CREATE operations on server principals
Audit Server Scope GDR	SQL Server 2005 and later	Records all GRANT, REVOKE, or DENY actions on permissions for executing T-SQL statements that change the server scope, such as creating a login
Audit Statement Permission	SQL Server 2000 only	Records when a user is authorized to execute a T-SQL statement on the registered SQL Server instance In SQL Server 2005 and later, this event class is Audit Database Management

SQL Compliance Manager monitor, audit and alert on SQL user activity and data changes.

IDERA | Products | Purchase | Support | Community | Resources | About Us | Legal