

Configuration wizard - Database level Privileged Users Audited Activity window

The Database Level Privileged Users Audited Activity window of the Configuration wizard allows you to specify which activities (events) you want to audit when the selected privileged users perform certain actions. You can choose to audit user defined events using IDERA SQL Compliance Manager. A user-defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

For example, you can audit all activities or only the activities related to specific types of events and actions, such as logins or database modifications (DMLs).

You can also audit activities that either failed or passed the required access check. For example, auditing failed activities allows you to track when a privileged user attempts to execute an action for which the login does not have the appropriate permissions.

Select the activities you want to audit, and then click **Next**.

The screenshot shows the 'SQLcm Configuration Wizard - Apply Regulation' window. The title bar includes a green checkmark icon, the text 'SQLcm Configuration Wizard - Apply Regulation', and standard window controls. The main content area is titled 'Database Level Privileged User Audited Activity' with the instruction 'Select which activities to audit for privileged users at database level.' Below this, there are two radio buttons: 'Audit all activities done by privileged users' (unselected) and 'Audit selected activities done by privileged users' (selected). Under the selected option, there is a list of activities with checkboxes: Logins, Logouts, Failed logins, Security changes, Administrative actions, Filter events based on access check: (with 'Passed' selected and 'Failed' unselected), Capture SQL Statements for DML and SELECT activities, Capture Transaction Status for DML Activity, and Capture SQL statements for DML and Security Changes. To the right of these, there are additional checkboxes for Database Definition (DDL), Database Modification (DML), Database SELECT operations, and User Defined Events. At the bottom of the window, there are three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Cancel'. On the left side of the window, there is a blue vertical bar with a 3D server icon.

Available actions

Audit all activities done by privileged users

Allows you to audit all activities involving your privileged users.

Audit selected activities done by privileged users

Allows you to select the privileged user activities you want audited.

Available fields

Audited Activity

Allows you to specify which activities (events) you want to audit for the selected privileged users.

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture transaction status for DML activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.