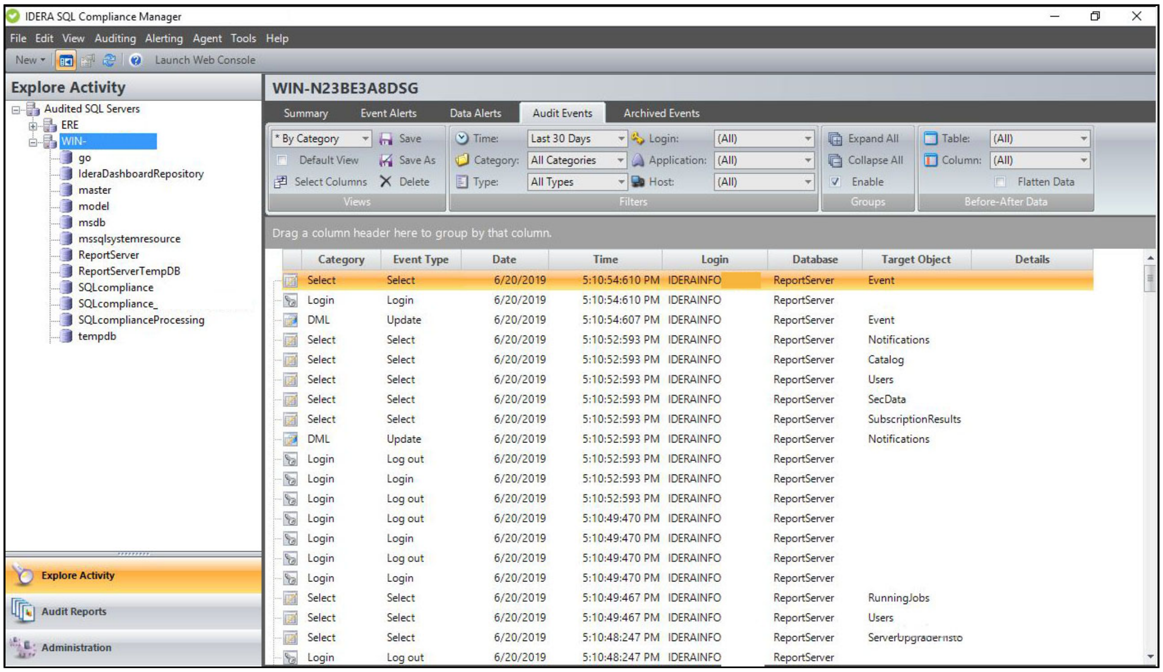
Audit Events tab

The Audit Events tab allows you to sort and analyze SQL events collected from the SQL Server instances and databases you are auditing.



View: By Category
Time: Last 30 Days
Category: All Categories
Type: All Types
Login: (All)
Application: (All)
Host: (All)
☑ Enable
Table: (All)
Column: (All)
☐ Flatten Data

Category	Event Type	Date	Time	Login	Database	Target Object	Details
Select	Select	6/20/2019	5:10:54:610 PM	IDERAINFO	ReportServer	Event	
Login	Login	6/20/2019	5:10:54:610 PM	IDERAINFO	ReportServer		
DML	Update	6/20/2019	5:10:54:607 PM	IDERAINFO	ReportServer	Event	
Select	Select	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	Notifications	
Select	Select	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	Catalog	
Select	Select	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	Users	
Select	Select	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	SecData	
Select	Select	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	SubscriptionResults	
DML	Update	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer	Notifications	
Login	Log out	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer		
Login	Login	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer		
Login	Log out	6/20/2019	5:10:52:593 PM	IDERAINFO	ReportServer		
Login	Log out	6/20/2019	5:10:49:470 PM	IDERAINFO	ReportServer		
Login	Login	6/20/2019	5:10:49:470 PM	IDERAINFO	ReportServer		
Login	Log out	6/20/2019	5:10:49:470 PM	IDERAINFO	ReportServer		
Login	Login	6/20/2019	5:10:49:470 PM	IDERAINFO	ReportServer		
Select	Select	6/20/2019	5:10:49:467 PM	IDERAINFO	ReportServer	RunningJobs	
Select	Select	6/20/2019	5:10:49:467 PM	IDERAINFO	ReportServer	Users	
Select	Select	6/20/2019	5:10:48:247 PM	IDERAINFO	ReportServer	ServerUpgradeHisto	
Login	Log out	6/20/2019	5:10:48:247 PM	IDERAINFO	ReportServer		

Available actions

View Before-After data

Allows you to view before and after data for DML events, according to the affected table or column. You can also change the display from a multi-level grid to a flat grid by clicking **Flatten Data**.

For more information about collecting before and after data, see the Before-After Data tab on the Audited Database Properties window.

Page through events

Allows you to page through the list of audited events. Use the previous and next arrows to navigate from page to page, up and down the list.

Create customized view

Allows you to create a custom version of this tab. You can change the data that is displayed by selecting different columns. You also can save your customizations to view later.

Filters

Allows you to filter the listed events by time span (for example, last seven days) or event category (for example, security).

Enable Groups

Allows you to group events by a specific property, such as the audited SQL Servers affected by the events or the times the events occurred. Enable groups when you want to sort the events or focus on a particular event attribute.

Refresh

Allows you to update the events list with current data.

Event Properties

Allows you to view details about the selected event.

Default columns

Icon

Provides a visual indication of the event category associated with the event so you can quickly scan the listed events for a specific type, such as a security event.

Category

Provides the name of the event category. The event category corresponds to the activity you are auditing. For example, if you are auditing EXECUTE events on stored procedures, the event category is DML.

Event

Provides the type of event that occurred.

Date

Provides the date that the event occurred.

Time

Provides the time that the event occurred.

Login

Provides the name of the SQL login that applied the change, using the format DomainName\LogonName.

Database

Provides the name of the database on which the event occurred.

Target Object

Provides the name of the database object targeted by the T-SQL statement associated with this event.

Details

Provides the text description of the event.

Before-After audit columns

Action

Provides the type of DML event that caused the table column to change (UPDATE, INSERT, or DELETE).

Date

Provides the date that the change occurred.

Time

Provides the time that the change occurred.

Columns Updated

Provides the number of columns that were changed by this event.

Audited Updates

Provides the number of updated columns for which audit data was collected. To collect different data, change audit settings.

Primary Key

Provides the name of the column that uniquely identifies this table. For more information about primary keys, see Microsoft Books Online.

Table

Provides the name of the table affected by this event.

After Value

Provides the value before this column was changed.

Before Value

Provides the value after this column was changed.

Column

Provides the name of the column affected by the event.

Row Count

Provides the frequency of data access.

Login

Provides the name of the SQL login that applied the change, using the format DomainName\LogonName.

Sensitive Column audit columns

Action

Displays the SELECT event that read the table column.

Application

Provides the name of the application that initiated this event.

Database

Provides the name of the database on which the event occurred.

Date

Provides the date that the change occurred.

Time

Provides the time that the change occurred.

Column

Provides the name of the column affected by the event.

Row Count

Provides the frequency of data access.

Login

Provides the name of the SQL login that read the column, using the format DomainName\LogonName.

Host

Provides the name of the computer where the event was initiated.

Additional columns

You can add any of these columns to this tab using the **Select Column** action. After you add a new column, you can save the tab as a custom view to reference later.

Access Check

Indicates whether this event passed or failed the SQL Server access check.

Application

Provides the name of the application that initiated this event.

Database User

Provides the name of the database user who executed this event.

Host

Provides the name of the computer where the event was initiated.

Object

Provides the name of the database object affected by this event.

Owner

Provides the name of the owner of the database affected by this event.

Privileged User

Indicates whether the user who initiated this event was a privileged user.

Role

Provides the type of SQL Server role assigned to the user who initiated this event.

Server

Provides the name of the SQL Server affected by this event.

Session Login

Provides the login credentials used to open the corresponding session with SQL Server.

SPID

Provides the SQL Server internal process ID of the object affected by the event.

Target Login

Provides the name of the SQL Server login targeted by the T-SQL statement associated with this event.

Target User

Provides the name of the database user targeted by the T-SQL statement associated with this event.