

# SQL Sentry Portal Alerts Log

Last Modified on 18 January 2023

## In this article:

- [Overview](#)
- [Alerts Log](#)
- [Alerts Details](#)
- [Filtering Alerts](#)
  - [Filtering alerts with the Top 5 charts](#)
  - [Filtering with the Search bar](#)
- [Adding, Editing, and Deleting Notes](#)
  - [Buttons](#)
  - [Grid Options](#)

## Overview

The SQL Sentry Portal delivers a workable set of alerts that have been carefully chosen by experienced Microsoft data platform professionals for their relevance to most database monitoring situations. The **Alerts Log** displays a list of all of the conditions in your SQL Sentry environment that have evaluated to *True*.

From the **Alerts Log**, you can sort and filter current and active alerts across your environment monitored by SQL Sentry. View the most recent 15 alerts by default or dig deeper into previously recorded alerts. With **Versions 2022.4 and later**, you can assign a user to an active alert directly from the Alerts Log, add/edit notes on selected alerts, and close out alerts.

## Alerts Log

The screenshot shows the SQL Sentry Alerts Log interface. The sidebar on the left contains navigation options: Health Overview, Alerts Log (selected), Dashboards, and Targets. The main content area is titled 'SQUADB-STABLE2' and features three donut charts: 'Top 5 Servers', 'Top 5 Conditions', and 'Top 5 Tags'. Below the charts is an 'Alerts Log' table with a search bar and a 'Clear' button. The table has columns for 'Close', 'Target', 'Type', 'Name', 'Condition Type', 'Action Type', 'Severity', 'Top 5', 'Assigned User', and 'Start Time'. The table lists several alerts, including 'managedinstance-qa-eus-mi-25b266ef096c.database.windows.net' and 'Q-REGRESSION.eng.local'.

**Note:** The default view on the **Alerts Log** page displays the 15 most recent alerts logged across your

environment (**Start Time** ↓). You can sort the table by any of the available columns.

The following Alerting information is displayed on the Alerts Log grid:

Column	Description
<b>Top 5 Servers</b>	The top 5 servers by alert count in real-time, or across the selected timeframe.
<b>Top 5 Conditions</b>	The top 5 conditions by alert count in real-time, or across the selected timeframe.
<b>Top 5 Tags</b>	The top 5 tags by alert count in real-time, or across the selected timeframe.
<b>Close</b>	Select the checkbox to close out the selected alert. Select the ▼ button to filter by the alert resolution status.
<b>Target</b>	The covered area of the watched <u>target</u> that triggered the alert. <b>Note:</b> If the scope of the target is at the server or instance level (i.e. Q-REGRESSION and not Q-REGRESSION: SQL Server Agent Jobs), then it will be a hyperlink to display <a href="#">Health</a> , <a href="#">Performance</a> , <a href="#">Top SQL</a> , <a href="#">Blocking</a> , <a href="#">Deadlocks</a> , or <a href="#">TempDB</a> for that target).
<b>Type</b>	The alert type, such as SQL Server, a deadlock (Deadlocks: Deadlock), etc.
<b>Name</b>	The name of the alert.
<b>Condition Type</b>	Conditions can fall into the General, Audit, Failsafe, and Advisory categories. For more information about the types of conditions categorized by SQL Sentry, see the <a href="#">General Conditions</a> , <a href="#">Audit Conditions</a> , <a href="#">Failsafe Conditions</a> , and <a href="#">Advisory Conditions</a> articles. Select the ▼ button to filter by specific condition types.
<b>Action Type</b>	The action that is set to occur once the monitored condition has been met. Actions are configured in the SQL Sentry client in the Conditions pane. For more information about configuring actions, and the available actions in SQL Sentry, see the <a href="#">Actions</a> article. Select the ▼ button to filter by specific action types.
<b>Assigned User</b>	The user or group assigned to the alert. If a user or group has not been assigned, select the drop-down menu and select the user or group you want to assign. You can also search for a user or group with the drop-down search bar.
<b>Severity</b>	The severity may be high, medium, or low. For more information about alert severity within SQL Sentry, see the <a href="#">Alert Severity</a> article. Select the ▼ button to filter by specific severity levels.
<b>Start Time</b>	The time the alert started evaluating to <i>true</i> .

Column	Description
<b>End Time</b>	The time the alert stopped evaluating to <i>true</i> .
<b>Duration</b>	The amount of time that the alert was <i>true</i> . <b>Note:</b> The smallest value displayed is in seconds. If an alert was active for 500ms, it would display a duration of <i>&lt; 1s</i> .
<b>Notes</b>	Add, edit, or delete notes for a selected alert. See the Notes section below for more information.

## Alerts Details

```
Alert Details | Q-REGRESSION.eng.local | 2022-10-13 10:37:01 AM

10/13/2022 10:37:01 AM -> Step 1 [process]
Executed as user: INTERCERVE\buildsvc. Microsoft.AnalysisServices.Xmla.ConnectionException: A connection cannot be made. Ensure that the server is running. ----> System.Net.Sockets.SocketException: No such host is known at System.Net.Sockets.TcpClient..ctor(String hostname, Int32 port) at Microsoft.AnalysisServices.Xmla.XmlaClient.GetTcpClient(ConnectionInfo connectionInfo) --- End of inner exception stack trace --- at Microsoft.AnalysisServices.Xmla.XmlaClient.GetTcpClient(ConnectionInfo connectionInfo) at Microsoft.AnalysisServices.Xmla.XmlaClient.OpenTopConnection(ConnectionInfo connectionInfo) at Microsoft.AnalysisServices.Xmla.XmlaClient.OpenConnection(ConnectionInfo connectionInfo, Boolean& isSessionTokenNeeded) at Microsoft.AnalysisServices.Xmla.XmlaClient.Connect(ConnectionInfo connectionInfo, Boolean beginSession) at Microsoft.SqlServer.Management.Smo.Olap.SoapClient.Connect() at OlapEvent(SCH_STEP* pStep, SUBSYSTEM* pSubSystem, SUBSYSTEMPARAMS* pSubSystemParams, Boolean kQueryFlag).

-----
[Connection] Q-REGRESSION.ENG.LOCAL
[Object Name] Process Sales Data
[Message] Job 'Process Sales Data' Failed on Step 1 [process]
[Start Time] 10/13/2022 10:37:01 AM
[End Time] 10/13/2022 10:37:01 AM
[Duration] 0 seconds

-----
[View in SQL Sentry Client]
url:sqlsentry:SQUADB-STABLE2\SentryOne/tem/eventview?c=19&id=1252034

-----
[Description] No description available.
[Owner] sa
[Category] [Uncategorized (Local)]
[Timestamp (Local)] 10/13/2022 10:37:36 AM
[Timestamp (UTC)] 10/13/2022 2:37:36 PM
[Generated By] SolarWinds SQL Sentry 2022.4 Server [SQUADB-STABLE2]
[Version] 2022.4.0.37137
[Monitor Type] EventHistoryMonitor
[Condition] SQL Server Agent Job Failure
[Response Ruleset] Notify Every Time (default)
[Configured Object Name] Global
[Configured Object Type] Global
```

The details logged for any selected alert are displayed on Alert details screen below the Alerts Log grid.

The alert window displays a **Severity** at the top. Only alerts with a **Category** of Advisory Conditions have an associated severity level. The severity levels may be *High*, *Medium*, or *Low*.

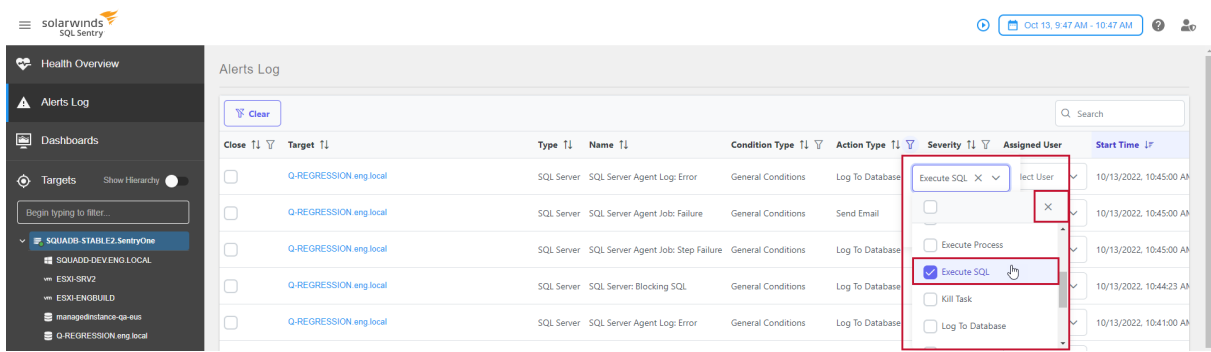
The available details vary depending on the condition, and may contain information such as the step of a failed SQL Server Agent job and the error behind the failure.

On an alert such as *High CPU*, which looks for CPU greater than 90, the performance counter value collected at the time of the alert evaluation is included (e.g. Performance Counter: Processor Information: % Processor Time, Total [97.4264] > [90] \*TRUE\* ).

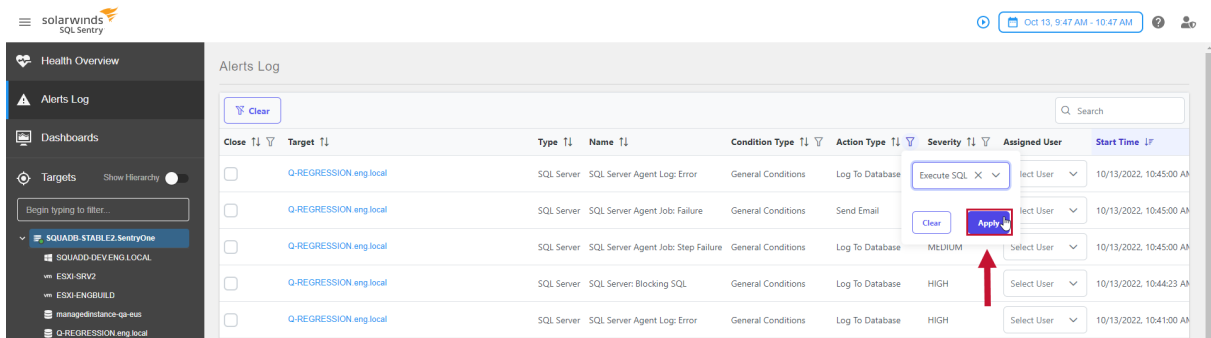
## Filtering Alerts

You can filter the alerts log by the Close, Condition Type, Action Type, or Severity categories; or you can filter by a combination of those categories. Filter the Alerts Log by completing the following steps:

1. Select the ▼ button for the desired category to open the filter drop-down menu.
2. Select the options you would like to filter by, and then select the ✕ icon to close the list of options.



3. Select **Apply** to apply your filter.

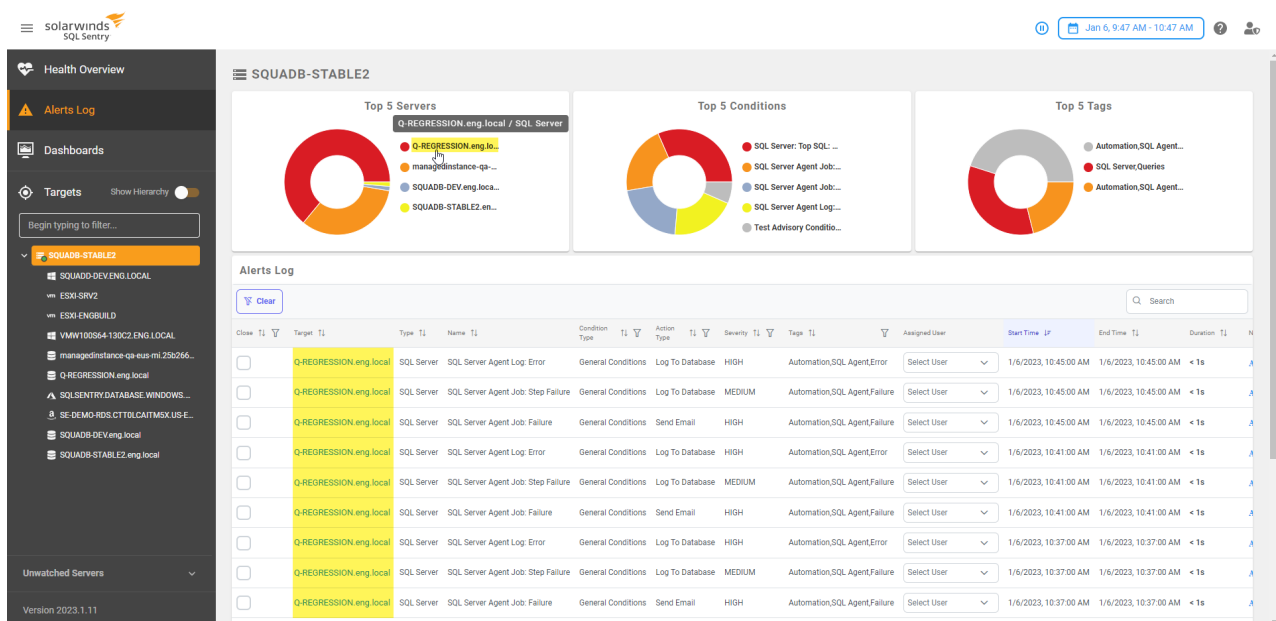


4. Repeat the steps above for any additional categories.

**Note:** Select the **Clear** button at the top of the Alerts Log to clear any filter.

## Filtering alerts with the Top 5 charts

Select an option from any of the Top 5 charts to filter the Alerts Log by your selection. For example, in the image below we selected Q-Regression from the Top 5 Servers chart to filter by the Q-Regression server.



## Filtering with the Search bar

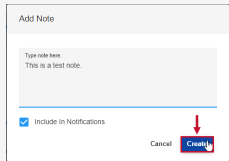



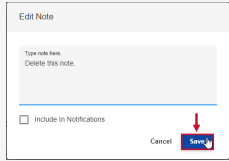


Use the search bar to further filter your Alerts Log. Type your search parameters into the search bar and select enter to filter the Alerts Log.

## Adding, Editing, and Deleting Notes

Starting with Versions 2022.4 and later, you can add, edit, and delete notes for any given alert using the Alerts Log grid.

Select **Add/View Notes** to open the Note Text column in the Alerts Log grid. The following options are available:

### Buttons

Button	Description	Image
<b>Add</b>	Select Add to open the Add Note window. Enter the text for your note in the textbox and then select Create to save your note.  <b>Note:</b> Select Include in Notifications to include your note in the alert notification.	
<b>Include In Notifications</b>	Indicates whether this note is included in alert notifications. A checkmark means the note is included.	
	Select  to open the Edit Note window. Enter the text for your note in the textbox and then select Save to save your note.	
	Select  to open the Delete Note window. Select Delete to permanently delete the note.	

**Note:** A prompt displays when you have successfully added, edited, or deleted a note.



### Grid Options

Option	Description

<b>Option</b>	<b>Description</b>
<b>Note Text</b>	A sample of the note text.
<b>Username</b>	The username that logged the note.
<b>Log Time</b>	The date and time the note was added or edited.