Use Status Alerts to ensure compliance

You can use Status Alerts to identify issues and potential disruptions in your IDERA SQL Compliance Manager deployment. By enabling Status Alerts, you can:

- Confirm that your SQL Server instances are available to be audited.
- Ensure the SQL Compliance Manager Agent and Collection Server are operating as expected.
- Proactively know when the event databases are growing too large so you can archive or groom your audit data before too much disk space is consumed.

Status Alerts best practices

Alert	What it means	What is the risk	What might be wrong
Agent cannot connect to audited instance	The SQL Compliance Manager Agent was unable to connect to the audited SQL Server instance. This alert is sent immediately after the failed connection occurs.	You are in danger of filling the trace directory and losing important audit data. Updated audit settings are not applied to the SQL trace that is collecting events, and you will fail to collect the events you want. SQL Server continues to write trace files to the SQL Compliance Manager Agent trace directory, but the agent cannot send these files to the Collection Server. When the trace directory is full, auditing ceases, impacting SQL Server performance. ***If the database id changes***, the agent will not be able to detect this update, causing the SQL trace to stop. ***If communications between the agent and the instance are "down" for more than 7 days***, the SQL trace automatically stops.	• The audited SQL Server instance may be offline or unable to respond. • The SQL Compliance Manager Agent service account does not have the required permissions to access the target SQL Server instance.
Agent heartbeat was not received	The Collection Server has not received a heartbeat from the SQL Compliance Manager Agent within the specified heartbeat interval.	Auditing is not immediately affected by this issue; however, you cannot apply updated audit settings. Trace files continue to queue in the trace file directory until the SQL Compliance Manager Agent Service is able to send these trace files to the Collection Server.	• The computer hosting the SQL Compliance Manager Agent may be offline. • Network firewall settings may be blocking communication between the SQL Compliance Manager Agent and the Collection Server. • The SQL Compliance Manager Agent may be stopped.

Agent trace directory reached size limit	The trace directory folder on the SQL Server computer where the SQL Compliance Manager Agent is deployed has exceeded the disk space percentage allocated in the alert rule.	You are in danger of filling the trace directory and losing important audit data. When the trace directory reaches its specified maximum size, the SQL Compliance Manager Agent ceases auditing the target instances. The SQL traces stop, and no subsequent events are collected. The size of the trace directory could also impact the performance of the SQL Server instances on this computer.	• The Collection Server may be offline, preventing the SQL Compliance Manager Agent from sending the trace files. • Network firewall settings may be blocking communication between the SQL Compliance Manager Agent and the Collection Server. • Your audit settings may be collecting more SQL Server events than you expected. • SQL Server traffic may have unexpectedly increased, causing more events to be collected and resulting in larger trace files.
Collection Server trace directory reached size limit	The trace directory folder on the computer where the Collection Server is installed has exceeded the disk space limit specified in the alert rule.	You are in danger of filling the trace directory, which can impact the performance of the Collection Server, such as delaying alerts. In turn, a full trace directory on the Collection Server can cause the SQL Compliance Manager Agent trace directory to fill as the trace files queue up to be sent. When the SQL Compliance Manager Agent trace directory reaches its specified maximum size, the agent will cease auditing the target instances. The SQL traces stop, and no subsequent events are collected.	• You can manually stop the Collection Service and prevent trace file processing. • The Collection Service may be unable to access the Repository due to inadequate permissions or an offline Repository database. • Your audit settings may be collecting more SQL Server events than you expected. • A third-party application, such as an anti-virus scanner, may be preventing the Collection Service from accessing the trace directory.

Event database is too large	The event database for an audited SQL Server instance is larger than the size limit specified in the alert rule.	Large event databases can significantly impact the performance of the Repository, and the SQL Server instance hosting the Repository.	• Your audit settings may be collecting more SQL Server events than you expected. • SQL Server traffic may have unexpectedly increased, causing more events to be collected and resulting in larger trace files. • You may need to archive or groom events.

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

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