Explore Activity - Instance Summary tab

The SQL Compliance Manager Instance Summary tab displays the status of audit activity for a particular SQL Server instance in your environment. Use the statistics and graphs on this tab to quickly and easily identify server-level issues so you can continue to ensure the correct level of compliance.

Understanding Server Status

Status

Indicates whether SQL CM encountered any issues while auditing this SQL Server instance. ***If a system alert is triggered***, the status displays as critical. System alerts notify you when the health of your SQL CM deployment may be compromised. For more information, see the Activity Log tab.

Last Heartbeat

Provides the most recent date and time that the SQLcompliance Agent deployed for this instance contacted the Collection Server.

Last Archived

Provides the most recent date and time that events collected for this instance were archived.

Processed Events

Displays the number of audit events stored in the Repository event databases for the selected time span. This number does not include events previously archived or groomed.

Recent Alerts

Displays the number of alerts generated for events collected from this instance during the specified time span.

Understanding the Server Activity Report Card status

Each tab of the Server Activity Report Card provides an auditing status for the corresponding event category. You can use this status to help you determine whether you are effectively auditing events on this SQL Server instance.
You can also use auditing thresholds to display critical issues or warnings should a particular activity, such as privileged user events, be higher than expected. These thresholds can notify you about issues related to increased activity levels, such as a security breach, that may be occurring on this instance. Use thresholds to supplement the alert rules you have configured for this instance.

Status Type	Indication	Meaning
Audited without thresholds	gray check	This event category is being audited on instances in your environment but auditing thresholds have not been set for this event category. Consider setting audit thresholds so you can track peaks in activity and identify any suspicious events.
Critical	red icon	The event activity during the selected time span is higher than the defined critical threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.
OK	green check	This event category is being audited on instances in your environment and auditing thresholds have been set for this event category.
Not audited	red icon	This event category is not being audited on instances in your environment even though auditing thresholds have been set for this event category. To track this activity, change your audit settings to include the corresponding event category. To ignore this activity, disable the auditing threshold set for this event category.
Not audited and no thresholds set	gray circle	This event category is not being audited on any instances in your environment. Auditing thresholds have not been set for this event category. Review whether you need to audit and track this activity on any of your SQL Server instance.
Warning	yellow icon	The event activity during the selected time span is higher than the defined warning threshold. To see more information about this activity, navigate to the Audit Events tab and search for events in the event category that is flagged. You can view the detailed properties of an event by double-clicking the listed event.

Understanding the Server Activity Report Card tabs

The Server Activity Report Card tabs chart recent activity for each of the common audit event categories and provide the status of this registered SQL Server instance. This activity and status is calculated from the processed audit events stored in the Repository event databases for the selected time span.

Use the Report Card to track the rate of activity in specific event categories and identify when exceptional activity occurs. Auditing thresholds can also help you track and identify activity that could reflect a SQL Server performance or security issue. Using the yellow and red lines that display when warning and critical auditing thresholds are exceeded, you can pinpoint the exact time at which the violations occurred.

When reviewing the Report Card, consider guidelines such as the following tips:

- Too many alerts and failed logins can indicate serious issues
- A sudden spike in privileged user activity could indicate a security breach
- Setting your Overall Activity threshold at 20% above the benchmark activity can warn you when unexpected traffic or database growth occurs

To get more detailed information about a particular increase in activity, use the Recent Audit Events pane to see which events correlated to this activity.

Understanding Audit Configuration

The Audit Configuration pane provides a brief summary of the audit settings configured for the selected SQL Server instance.

For more detailed information, review the properties of the registered instance.

Server

Lists the event categories currently audited on this SQL Server instance. This list includes auditing settings configured at the server level.

Privileged Users

Displays the number of privileged users who are being audited, and the audit settings currently configured to track their activity.

Databases

Indicates the number of databases hosted by this SQL Server instance that are being audited.

Event Filters

Displays the number of Event Filters that have been created to streamline audit data collected from this SQL Server instance, and the event properties being used by these filters. Events that match the listed properties are omitted from the audit data trail for this instance.

Understanding Recent Audit Events

The Recent Audit Events pane lists the most recent audit events collected for this SQL Server instance during the specified time span. This list displays up to 100 events.

To see more details about a specific event, double-click the listed event.

To view all audited events collected since your last archive, use the Audit Events tab.

Available actions

Configure Alerting

Opens the Alert Rules tab under Administration, allowing you to configure alerting to track specific activity on this instance or other SQL Server instances across your environment.

Remove Server

Allows you to unregister the selected SQL Server instance. When you remove a SQL Server instance, SQL Compliance Manager disables all auditing at the server and database levels on the SQL Server instance. ***If the selected instance is the last instance to be audited on this SQL Server***, SQL CM also uninstalls the SQLcompliance Agent. ***If you manually deployed the SQLcompliance Agent***, you must manually uninstall it from the SQL Server computer.

Add Audited Databases

Starts the New Audited Database wizard, allowing you to enable auditing on additional databases hosted by this SQL Server instance.

Disable Auditing

Allows you to disable auditing on the selected SQL Server instance. When you disable auditing, the SQLcompliance Agent stops collecting new event data, and stops the corresponding SQL trace. You can continue to view and report on previously audited events or archived events.

To re-enable auditing, right-click the instance from the **Explore Activity** tree, and then click **Enable Auditing** on the context menu.

Server Settings

Allows you to change the audit settings for the selected SQL Server instance.

Apply Regulation Guideline

Allows you to select one or more regulations to apply to all of the audited databases within this SQL Server instance. If you want to apply regulation guidelines only to specific databases, use the **Apply Regulation Guideline** feature from the Explore Activity - Database Summary tab. This option is unavailable if you have no databases selected for audit.

Privileged Users

Allows you to change how privileged user activity is audited on the selected SQL Server instance.

Import

Allows you to import audit settings previously exported from another SQL Server instance. Using the Import Audit Settings wizard, you can specify whether you want to import settings at the server or database level.

Export

Allows you to export audit settings for this SQL Server instance to an XML file. This file includes audit settings configured at the server and database level. You can later use this file to import audit settings across multiple SQL Server instances, ensuring consistent auditing and compliance throughout your environment.

Collect Audit Data

Allows you to force the SQLcompliance Agent to send trace files to the Collection Server for processing. Typically, the SQLcompliance Agent sends trace files to the Collection Server at the specified collection interval. By default, a trace file collection occurs every two minutes.

Agent Properties

Allows you to view or change the properties, such as the heartbeat interval and the collection interval, of the SQLcompliance Agent deployed to the selected SQL Server instance.

Span

Allows you to change the number of days (time span) for which the Summary tab displays status, alerts, and activity. By default, this tab displays data for the last 7 days.