Overview of log queries in Azure Monitor

06/19/2019 • 5 minutes to read • +3

In this article

Log queries help you to fully leverage the value of the data collected in Azure Monitor Logs. A powerful query language allows you to join data from multiple tables, aggregate large sets of data, and perform complex operations with minimal code. Virtually any question can be answered and analysis performed as long as the supporting data has been collected, and you understand how to construct the right query.

Some features in Azure Monitor such as insights and solutions process log data without exposing you to the underlying queries. To fully leverage other features of Azure Monitor, you should understand how queries are constructed and how you can use them to interactively analyze data in Azure Monitor Logs.

Use this article as a starting point to learning about log queries in Azure Monitor. It answers common questions and provides links to other documentation that provides further details and lessons.

How can I learn how to write queries?

If you want to jump right into things, you can start with the following tutorials:

- Get started with Log Analytics in Azure Monitor.
- Get started with log queries in Azure Monitor.

Once you have the basics down, walk through multiple lessons using either your own data or data from our demo environment starting with:

- Work with strings in Azure Monitor log queries

What language do log queries use?

Azure Monitor Logs is based on Azure Data Explorer, and log queries are written using the same Kusto query language (KQL). This is a rich language designed to be easy to read and author, and you should be able to start using it with minimal guidance.

See Azure Data Explorer KQL documentation for complete documentation on KQL and reference on different functions available.
See Get started with log queries in Azure Monitor for a quick walkthrough of the language using data from Azure Monitor Logs. See Azure Monitor log query language differences for minor differences in the version of KQL used by Azure Monitor.

What data is available to log queries?

All data collected in Azure Monitor Logs is available to retrieve and analyze in log queries. Different data sources will write their data to different tables, but you can include multiple tables in a single query to analyze data across multiple sources. When you build a query, you start by determining which tables have the data that you're looking for, so you should have at least a basic understanding of how data in Azure Monitor Logs is structured.

See Sources of Azure Monitor Logs, for a list of different data sources that populate Azure Monitor Logs.
See Structure of Azure Monitor Logs for an explanation of how the data is structured.

What does a log query look like?

A query could be as simple as a single table name for retrieving all records from that table:

Kusto Copy

```
Syslog
```

Or it could filter for particular records, summarize them, and visualize the results in a chart:

Copy

```
SecurityEvent
| where TimeGenerated > ago(7d)
| where EventID == 4625
| summarize count() by Computer, bin(TimeGenerated, 1h)
| render timechart
```

For more complex analysis, you might retrieve data from multiple tables using a join to analyze the results together.

Kusto Copy

```
app("ContosoRetailWeb").requests
| summarize count() by bin(timestamp,1hr)
| join kind= inner (Perf
    | summarize avg(CounterValue)
      by bin(TimeGenerated,1hr))
on $left.timestamp == $right.TimeGenerated
```

Even if you aren't familiar with KQL, you should be able to at least figure out the basic logic being used by these queries. They start with the name of a table and then add multiple commands to filter and process that data. A query can use any number of commands, and you can write more complex queries as you become familiar with the different KQL commands available.

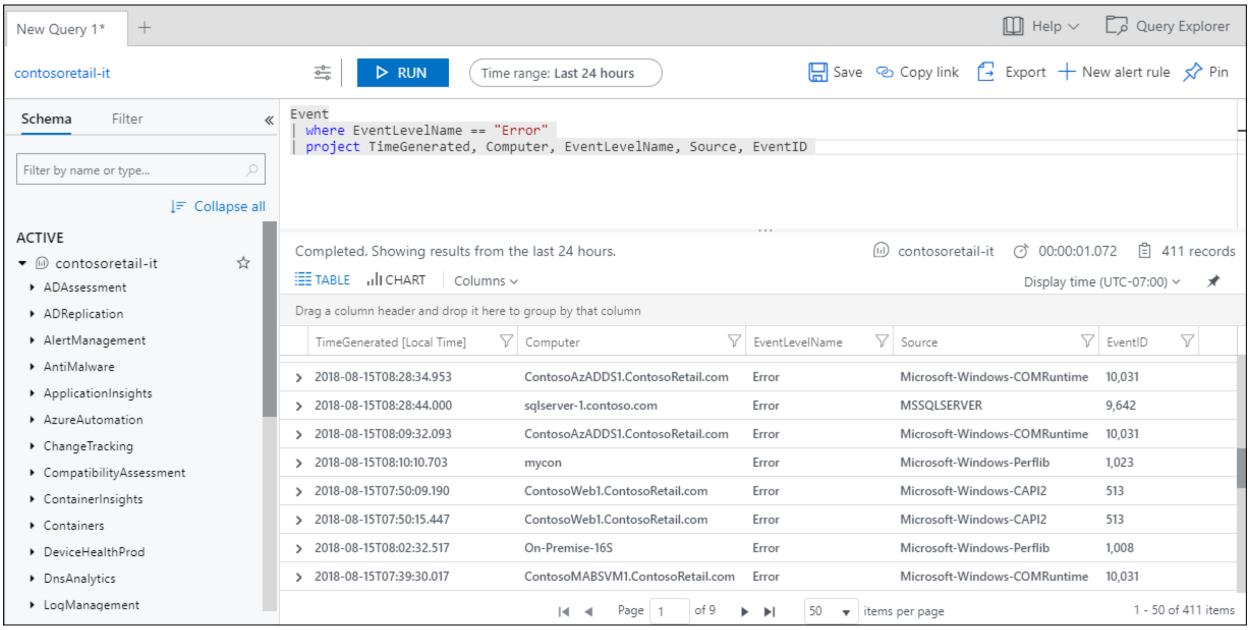
See Get started with log queries in Azure Monitor for a tutorial on log queries that introduces the language and common functions, .

What is Log Analytics?

Log Analytics is the primary tool in the Azure portal for writing log queries and interactively analyzing their results. Even if a log query is used elsewhere in Azure Monitor, you'll typically write and test the query first using Log Analytics.

You can start Log Analytics from several places in the Azure portal. The scope of the data available to Log Analytics is determined by how you start it. See Query Scope for more details.

- Select **Logs** from the **Azure Monitor** menu or **Log Analytics workspaces** menu.
- Select **Logs** from the **Overview** page of an Application Insights application.
- Select **Logs** from the menu of an Azure resource.



```
Event
| where EventLevelName == "Error"
| project TimeGenerated, Computer, EventLevelName, Source, EventID
```

Completed. Showing results from the last 24 hours. contosoretail-it 00:00:01.072 411 records

TimeGenerated [Local Time]	Computer	EventLevelName	Source	EventID
2018-08-15T08:28:34.953	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:28:44.000	sqlserver-1.contoso.com	Error	MSSQLSERVER	9,642
2018-08-15T08:09:32.093	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:10:10.703	mycon	Error	Microsoft-Windows-Perflib	1,023
2018-08-15T07:50:09.190	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T07:50:15.447	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T08:02:32.517	On-Premise-16S	Error	Microsoft-Windows-Perflib	1,008
2018-08-15T07:39:30.017	ContosoMABSVM1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031

See Get started with Log Analytics in Azure Monitor for a tutorial walkthrough of Log Analytics that introduces several of its features.

Where else are log queries used?

In addition to interactively working with log queries and their results in Log Analytics, areas in Azure Monitor where you will use queries include the following:

- **Alert rules.** Alert rules proactively identify issues from data in your workspace. Each alert rule is based on a log search that is automatically run at regular intervals. The results are inspected to determine if an alert should be created.
- **Dashboards.** You can pin the results of any query into an Azure dashboard which allow you to visualize log and metric data together and optionally share with other Azure users.
- **Views.** You can create visualizations of data to be included in user dashboards with View Designer. Log queries provide the data used by tiles and visualization parts in each view.
- **Export.** When you import log data from Azure Monitor into Excel or Power BI, you create a log query to define the data to export.
- **PowerShell.** You can run a PowerShell script from a command line or an Azure Automation runbook that uses Get-AzOperationalInsightsSearchResults to retrieve log data from Azure Monitor. This cmdlet requires a query to determine the data to retrieve.
- **Azure Monitor Logs API.** The Azure Monitor Logs API allows any REST API client to retrieve log data from the workspace. The API request includes a query that is run against Azure Monitor to determine the data to retrieve.

Next steps

- Walk through a tutorial on using Log Analytics in the Azure portal.
- Walk through a tutorial on writing queries.

Related Articles

- Get started with log queries in Azure Monitor
- Get started with Azure Monitor Log Analytics
- Azure Monitor log query examples
- Azure Monitor log queries

Recommendations are based on machine learning analysis and tuned by our content authors.

Is this page helpful?

Yes No