

# How query details on audit records - Log Analytics

Last updated by | Ricardo Marques | Mar 1, 2023 at 6:16 AM PST

## Contents

- [Context](#)
- [Steps to get the information](#)
- [Internal reference](#)

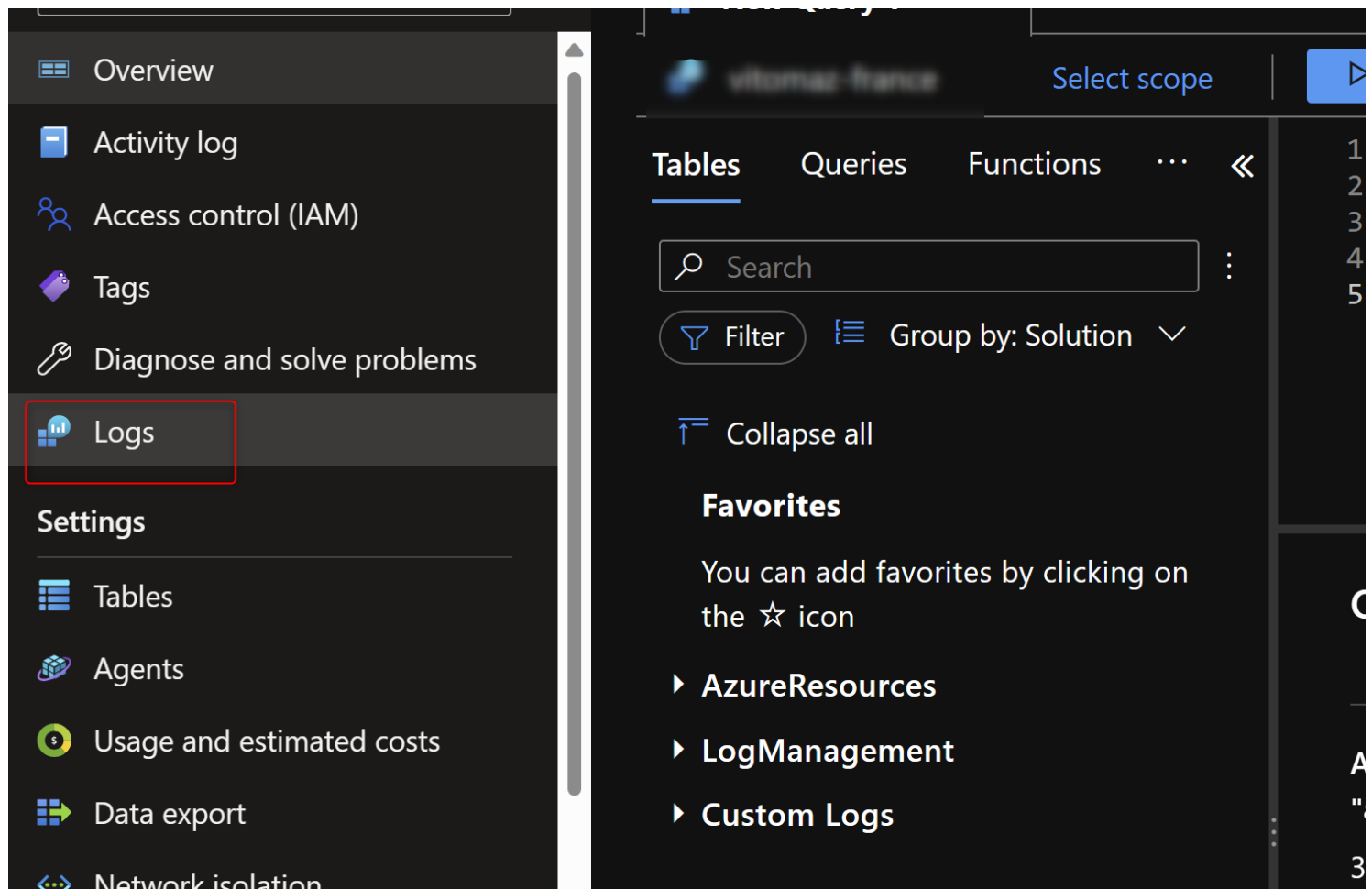
## Context

Customer has [auditing enabled](#) . The target is Log Analytics.

Server experiencing performance problems and wants to know how he can retrieve information about the user that executes that specific query.

## Steps to get the information

1 - Navigate to the Log Analytics Workspace. Under **General** choose **Logs**



2 - On the Query window run the query below (add output columns as many as you need. On this example I'm interested on the user, timestamp, query and client program used):

```
AzureDiagnostics
| where server_instance_name_s == "ServerName" //server name
| where database_name_s == "DatabaseName" //database name
| where statement_s contains "insert into large_table" //part of the statement that you are looking for
| where TimeGenerated > ago(15d) //time range
| project TimeGenerated, session_server_principal_name_s, server_instance_name_s, statement_s, application_name_s
```

On the example below I have the information about the user that inserted on the table and that he used SQL Server Management Studio:

Results Chart					
TimeGenerated [UTC]	session_server_principal_name_s	server_instance_name_s	statement_s	application_name_s	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	
> 2/22/2023, 2:04:40.658 PM	miadmin	server1	insert into large_table values ('a...	Microsoft SQL Server Management Studio - Quer	

Internal reference

[371109681](#) 

How good have you found this content?

