Events for table public.lsnmover table are constantly logged in Audit logs

Last updated by | Daniel Valero | Apr 7, 2022 at 2:03 PM PDT

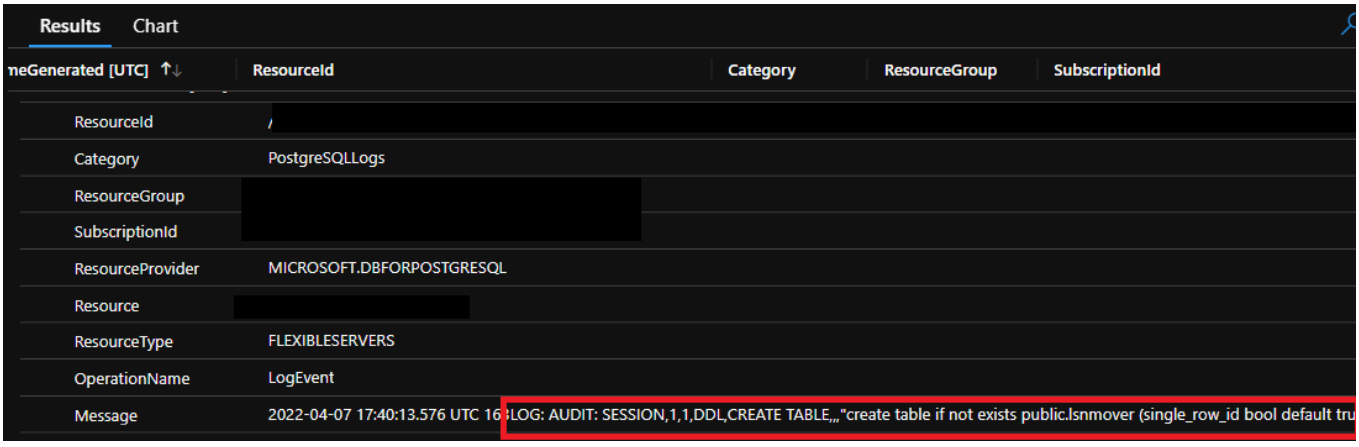
Contents

Issue

- When pgAudit is enabled and configured to capture DDL and/or ALL events, multiple events related to the creation of *public.lsnmover* table is logged.
    - If using an Storage Accounts as destination for the log you see:

> AUDIT: SESSION,1,1,DDL,CREATE TABLE,,,"create table if not exists public.lsnmover (single_row_id bool default true, id bigint, update_time timestamp default now(), constraint ensure_one_row CHECK (single_row_id), constraint lsnmover_pk primary key (single_row_id))"

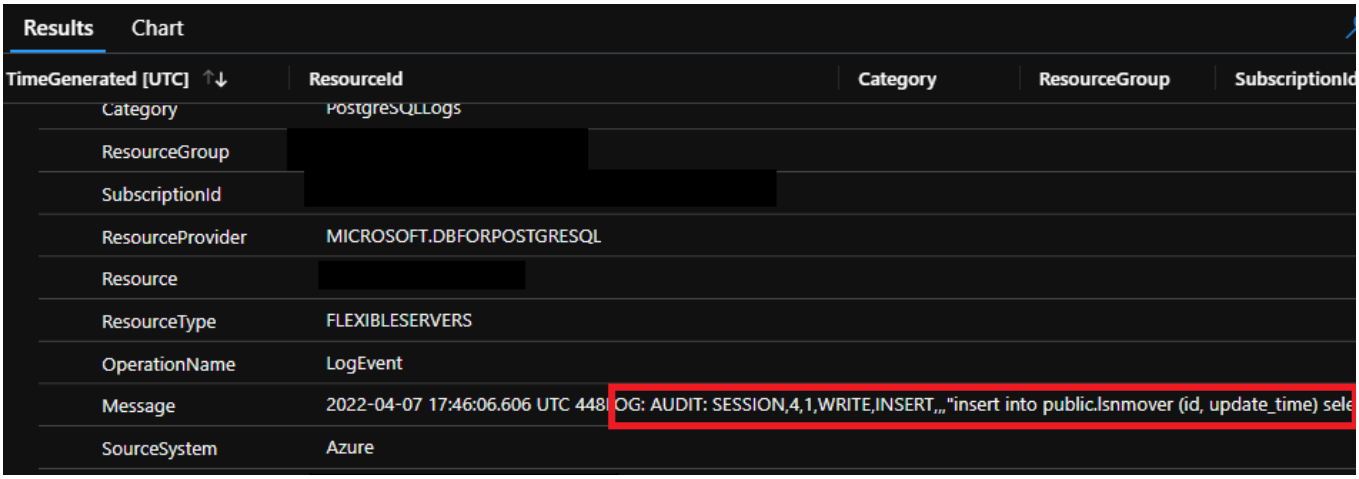
    - If using an Log Analytics Workspace as destination for the log you see:



- When pgAudit is enabled and configured to capture WRITE and/or ALL events, multiple events related to the creation of *public.lsnmover* table is logged as shown below:
    - If using an Storage Accounts as destination for the log you see::

> AUDIT: SESSION,2,1,WRITE,INSERT,,,"insert into public.lsnmover (id, update_time) select 1, now() on conflict on constraint lsnmover_pk do update set id = public.lsnmover.id+1, update_time=now()"

- If using an Log Analytics Workspace as destination for the log you see:



Investigation/Analysis

These log entries are generated by synthetic writes, and basically these synthetic writes are executed with some frequency to quickly detect when the server gets unhealthy.

Mitigation

There is a Work Item created for it https://msdata.visualstudio.com/Database Systems/_workitems/edit/1561683

No ETA for solution to be deployed yet. Need to check Work Item

RCA Template

These log entries are generated by synthetic writes, and basically these synthetic writes are executed with some frequency to quickly detect when the server gets unhealthy.

At this point we don't have an ETA on when the fix will be implemented and deployed.

More Information

You can ask the Cx to modify the parameter **log_line_prefix** to include the name of the user executing the command, for example to a value such as %m %p - user %u -

They then see then that the user executing the command is **azuresu** as shown in the example below:

> 2022-04-07 18:30:54.277 UTC 2699 - user azuresu - LOG: AUDIT: SESSION,4,1,WRITE,INSERT,,,"insert into public.lsnmover (id, update_time) select 1, now() on conflict on constraint lsnmover_pk do update set id = public.lsnmover.id+1, update_time=now()",<not logged>

Then, if they are using Log Analytics Workspace as destination for the log , they can exclude the operation from this user by adding the filter: **!contains "user azuresu"** as in the example below:

```
AzureDiagnostics
| where ResourceProvider =="MICROSOFT.DBFORPOSTGRESQL"
| where Category == "PostgreSQLLogs"
| where Message contains "AUDIT:" and Message !contains "user azuresu"
```

Internal Reference

- https://portal.microsofticm.com/imp/v3/incidents/details/279064235/home