LogAnalytics Alert for DDL operations on PostgreSQL example

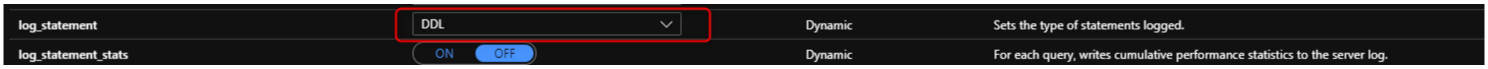
Last updated by | Lisa Liu | Nov 6, 2020 at 10:34 AM PST

If a customer wants to trigger alerts for DDL operations, for example CREATE TABLE, one way to achieve this is to send postgresql logs to log analytics and build the Alert based on a Log analytics query.

Note that on the example below, if the customer setup the alert on one server, if he wants to include a new server, if he uses the same log analytics workspace, he only needs to follow steps 1, 2 and 3.

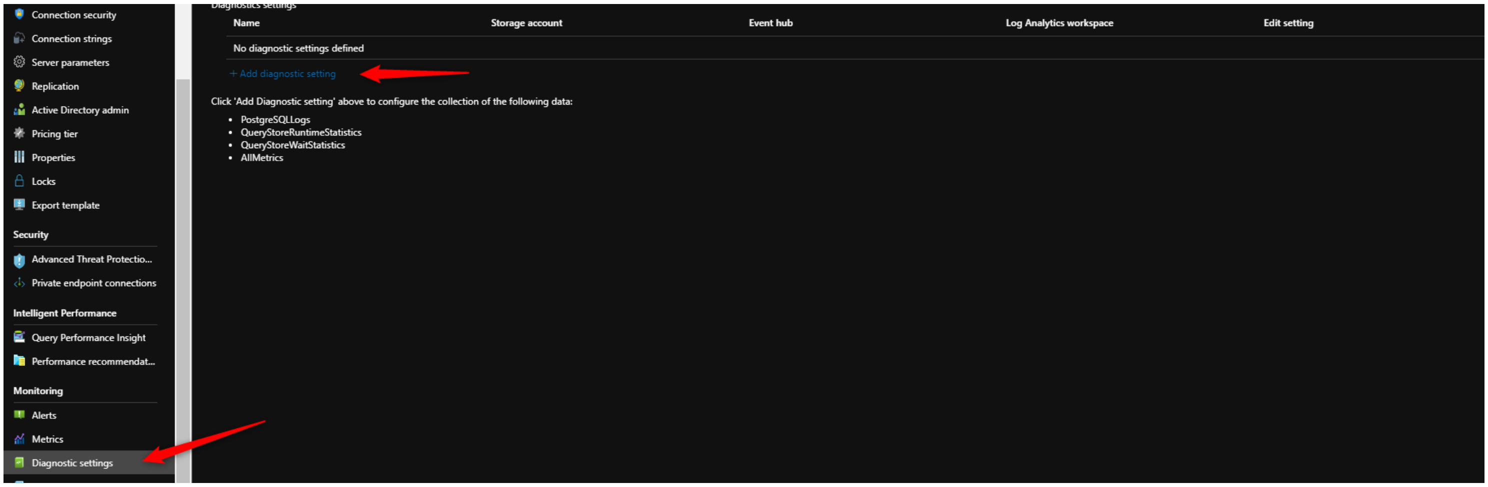
Basically we are going to send the postgresql logs to log analytics and build the alerts on top of a log analytics query, like so first of all you need to create a log analytics workspace: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace

1 – make sure that on the server parameters you are logging DDL statements



log_statement	DDL	Dynamic	Sets the type of statements logged.
log_statement_stats	ON OFF	Dynamic	For each query, writes cumulative performance statistics to the server log.

2 – on the server diagnostic settings, add a new diagnostic setting



Diagnostics settings

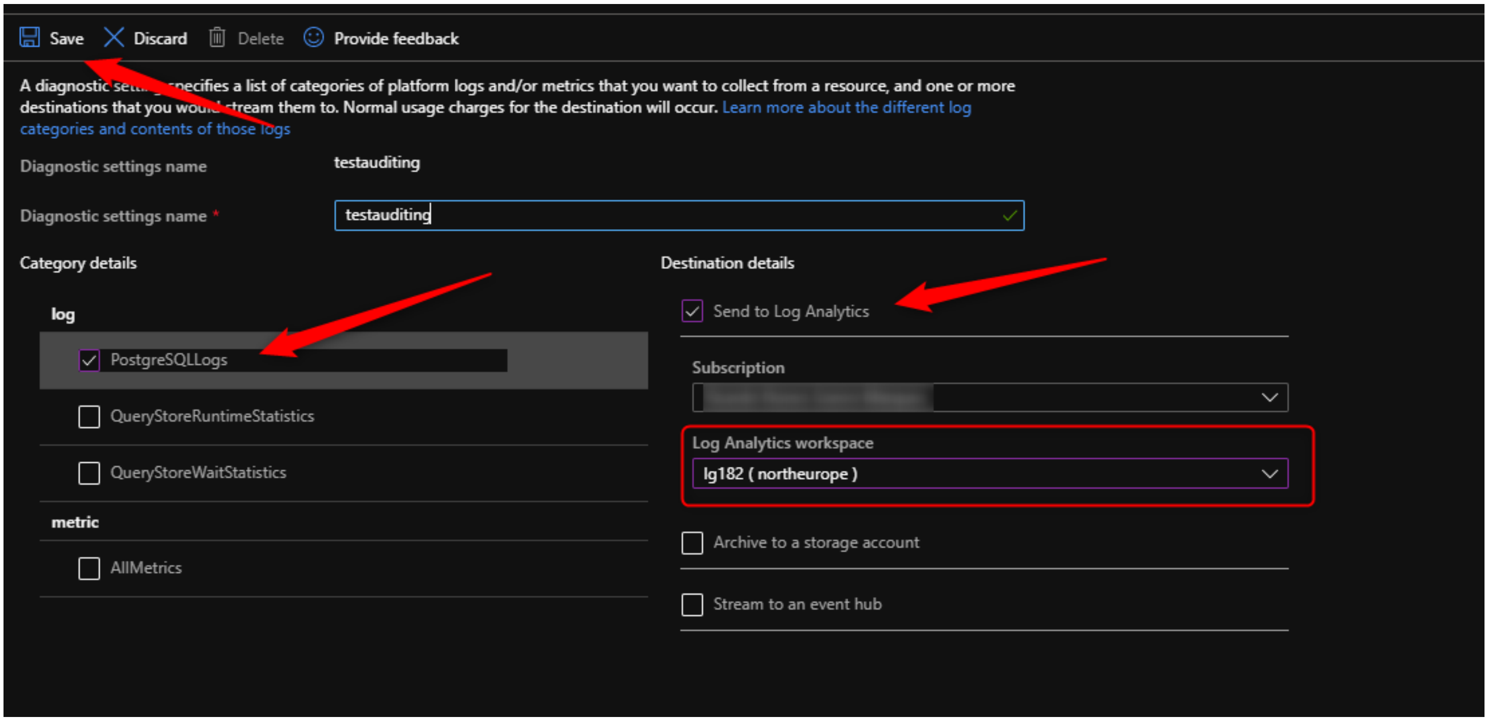
Name	Storage account	Event hub	Log Analytics workspace	Edit setting
No diagnostic settings defined				

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- PostgreSQLLogs
- QueryStoreRuntimeStatistics
- QueryStoreWaitStatistics
- AllMetrics

3 – send the PostgreSQLLogs to the log analytics workspace and click on Save:



A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic settings name testauditing

Diagnostic settings name * testauditing

Category details

log

☑ PostgreSQLLogs

□ QueryStoreRuntimeStatistics

□ QueryStoreWaitStatistics

metric

□ AllMetrics

Destination details

☑ Send to Log Analytics

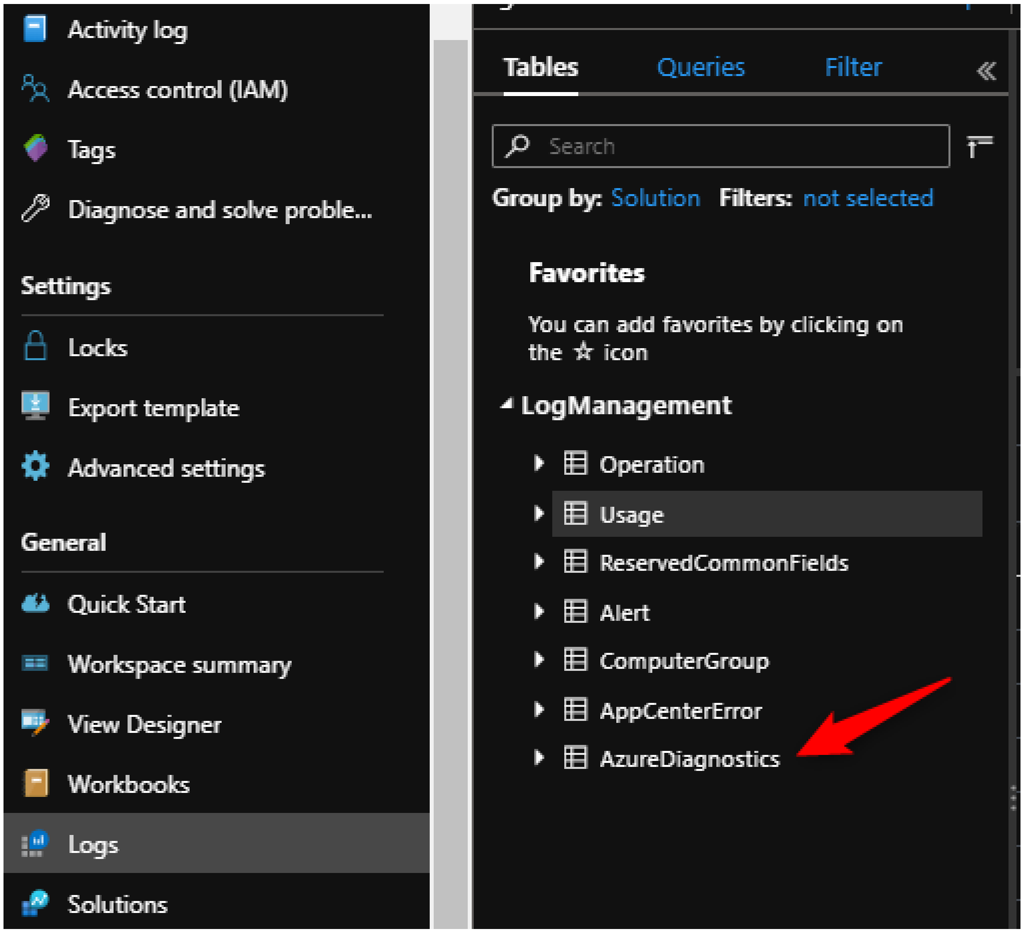
Subscription [redacted]

Log Analytics workspace lg182 (northeurope)

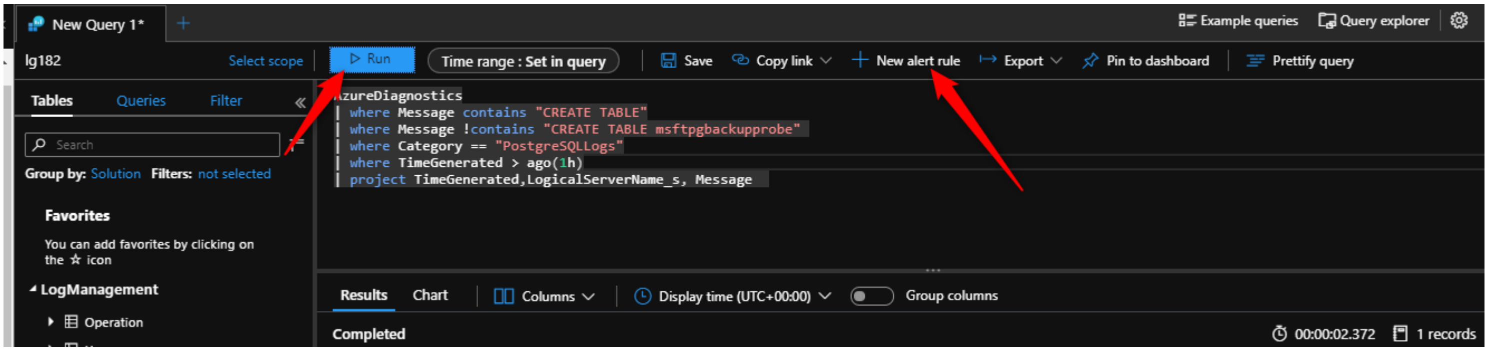
□ Archive to a storage account

□ Stream to an event hub

4 – Navigate to your Log Analytics workspace. On Logs section. A table named AzureDiagnostics should be visible (it should take some minutes to be available after the first setup):



5 – Copy and paste the query below into the query window and Run (even if doesn`t return any results). Then click on “New alert rule”

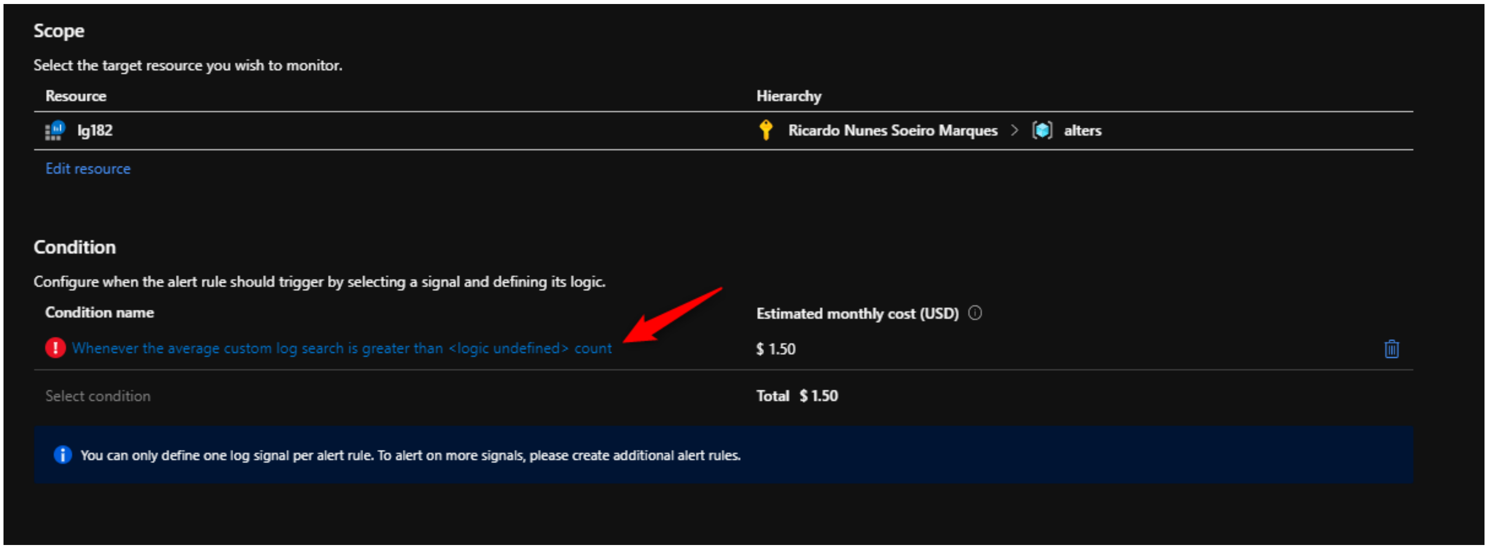


```
AzureDiagnostics
| where Message contains "CREATE TABLE"
| where Message !contains "CREATE TABLE msftpgbackupprobe"
| where Category == "PostgreSQLLogs"
| where TimeGenerated > ago(1h)
| project TimeGenerated,LogicalServerName_s, Message
```

AzureDiagnostics | where Message contains "CREATE TABLE" | where Message !contains "CREATE TABLE msftpgbackupprobe" | where Category == "PostgreSQLLogs" | where TimeGenerated > ago(1h) | project TimeGenerated,LogicalServerName_s, Message

Note – if you notice, Im not specifying any server name. I`m only looking for create tables executed by users in the last hour, inside postgresql logs. I will explain this below.

6 – on the Alert configuration, click on the Condition



Scope

Select the target resource you wish to monitor.

Resource	Hierarchy
lg182	Ricardo Nunes Soeiro Marques > alters

Edit resource

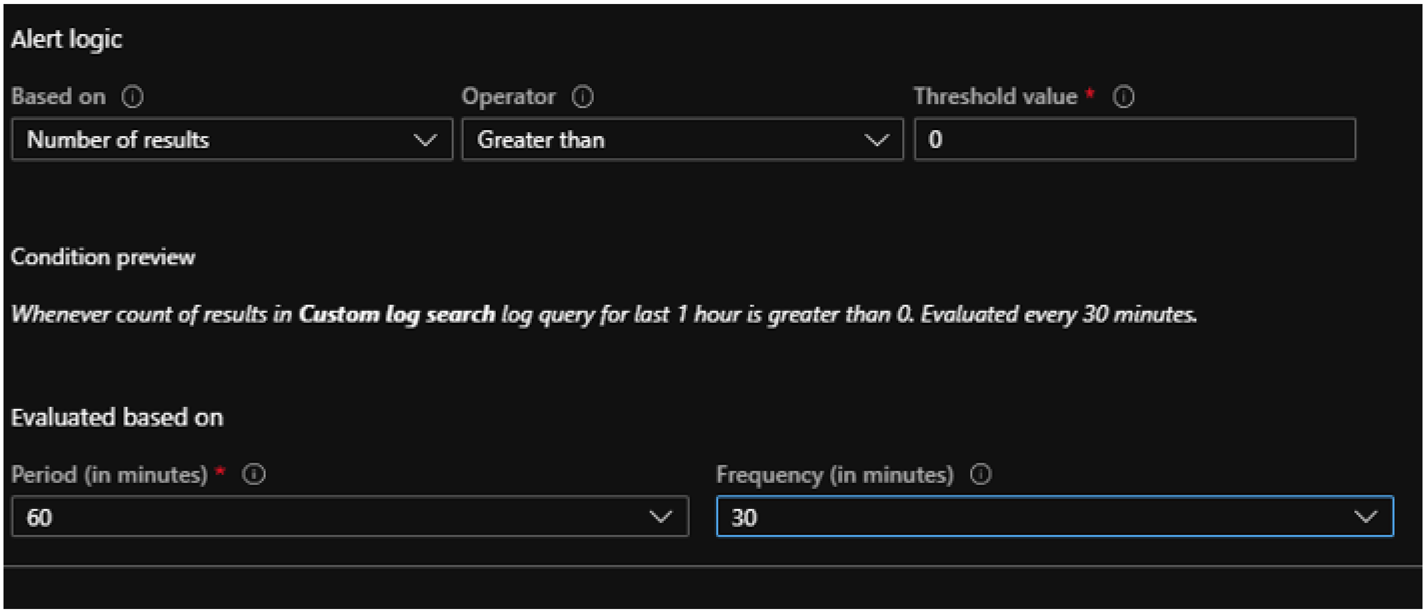
Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name	Estimated monthly cost (USD)
Whenever the average custom log search is greater than <logic undefined> count	$ 1.50
Select condition	Total $ 1.50

You can only define one log signal per alert rule. To alert on more signals, please create additional alert rules.

7 – set the condition logic (specify according with your needs) – I`m setting to trigger an alert every time I have a row for the query output. Then click on “Done”



Alert logic

Based on: Number of results

Operator: Greater than

Threshold value *: 0

Condition preview

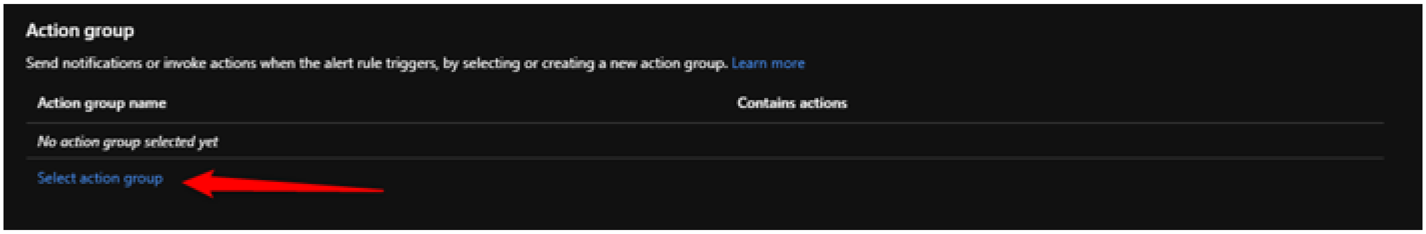
*Whenever count of results in **Custom log search** log query for last 1 hour is greater than 0. Evaluated every 30 minutes.*

Evaluated based on

Period (in minutes) *: 60

Frequency (in minutes): 30

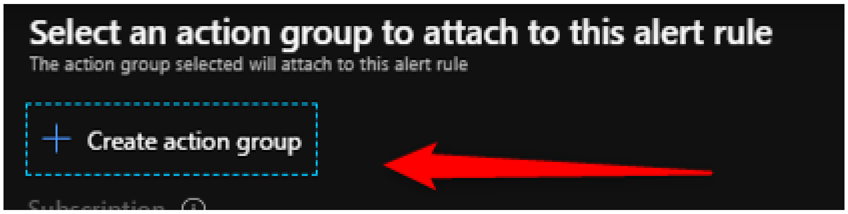
8 – create an Action group (if you don`t have one):



Action group

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. Learn more

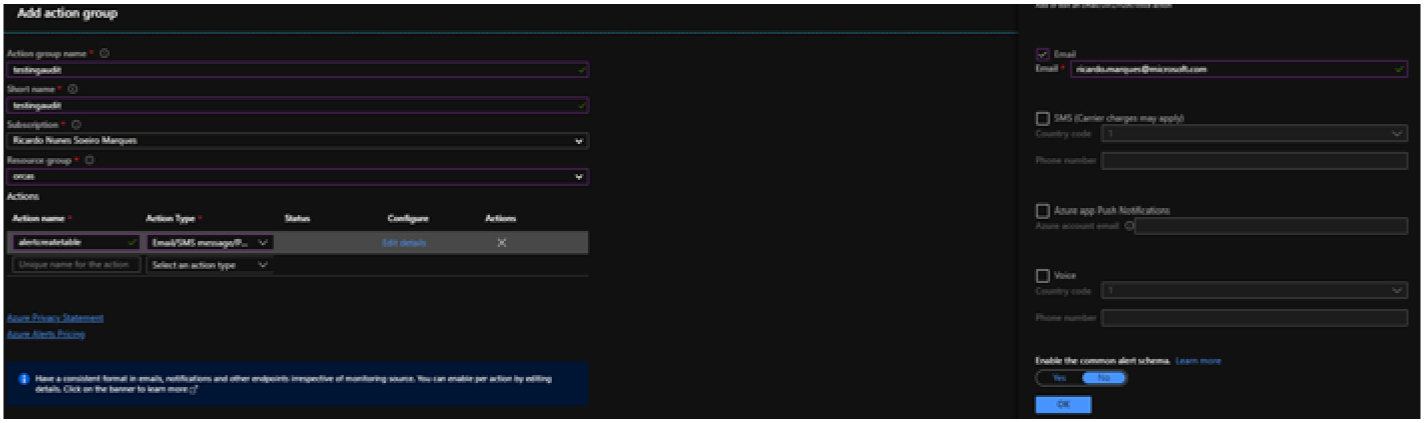
Action group name	Contains actions
No action group selected yet	



Select an action group to attach to this alert rule

The action group selected will attach to this alert rule

I`m creating one based on emails



Add action group

Action group name *: testingaudit

Short name *: testingaudit

Subscription *: Ricardo Nunes Soeiro Marques

Resource group *: orcas

Actions

Action name *	Action Type *	Status	Configure	Actions
alertcreatetable	Email/SMS message/P...		Edit details	✕
Unique name for the action	Select an action type			

Have a consistent format in emails, notifications and other endpoints irrespective of monitoring source. You can enable per action by editing details. Click on the banner to learn more

☑ Email

Email *: ricardo.marques@microsoft.com

□ SMS (Carrier charges may apply)

Country code: 1

Phone number:

□ Azure app Push Notifications

Azure account email:

□ Voice

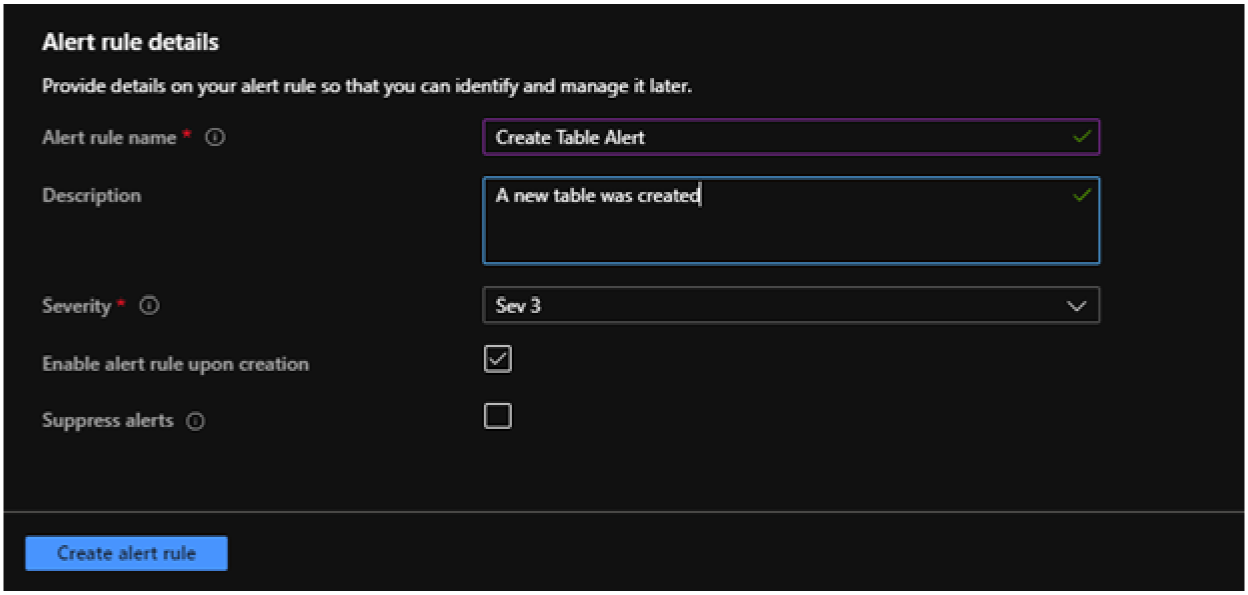
Country code: 1

Phone number:

Enable the common alert schema. Learn more

Yes [✓ No]

9 – configure the new alert details:



Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name * : Create Table Alert

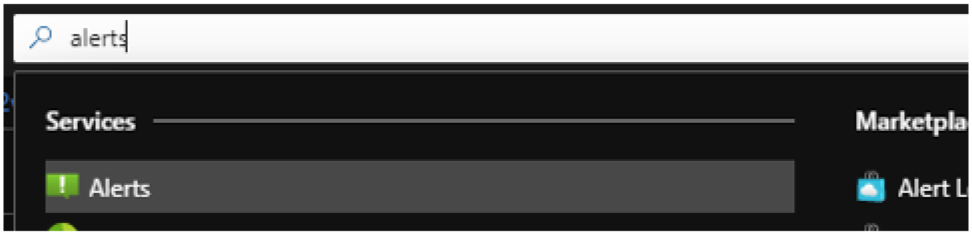
Description: A new table was created

Severity * : Sev 3

Enable alert rule upon creation ☑

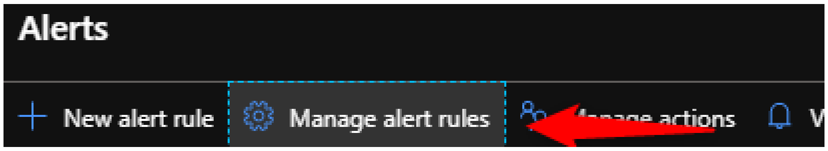
Suppress alerts ☐

10 – check the rule created. Type rules on the search box:

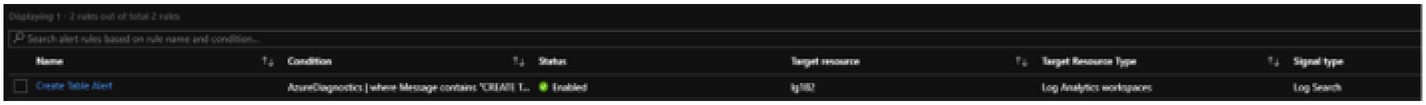


alerts

Click on Manage alert rules:



The alert appears



Displaying 1 - 2 rules out of total 2 rules

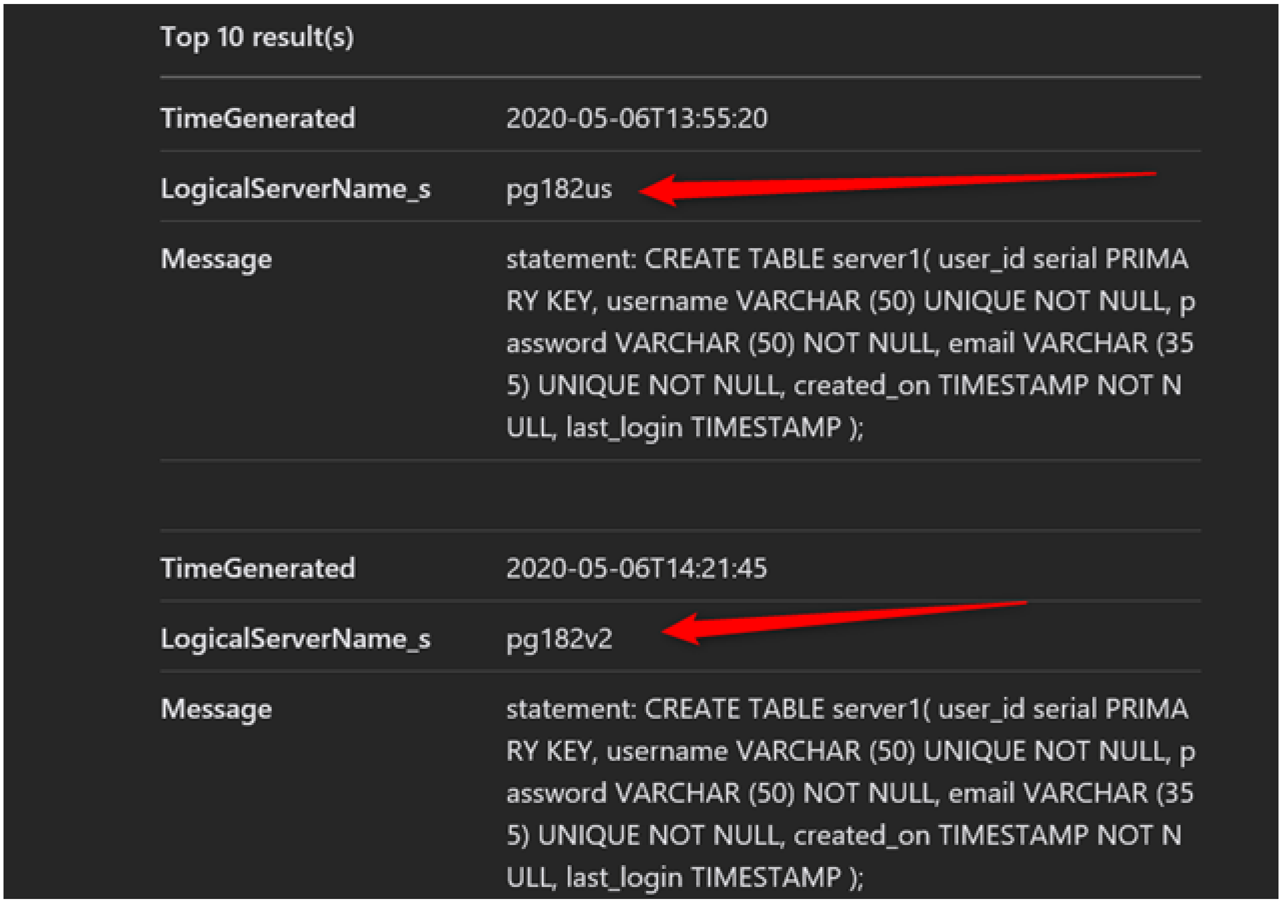
Search alert rules based on rule name and condition...

Name	Condition	Status	Target resource	Target Resource Type	Signal type
☐ Create Table Alert	AzureDiagnostics | where Message contains "CREATE T...	● Enabled	lg182	Log Analytics workspaces	Log Search

Note that the alert doesn`t use postgresql specifically. We are pointing to a Log analytics workspace.

Now, if I want to add the same alert for another portgresql server I just need to steps 1, 2 and 3 if I use the same log analytics workspace – the alert is already setup on the log analytics workspace.

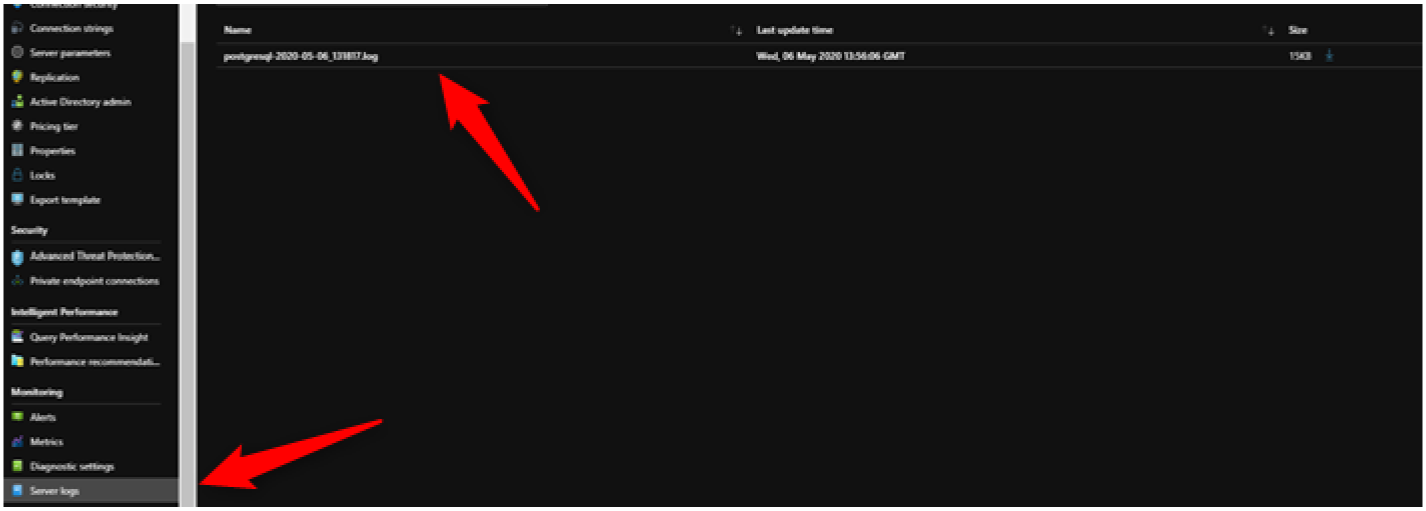
An example of an alert email triggered after creating one table of on two different servers, sharing the same alert:



Top 10 result(s)

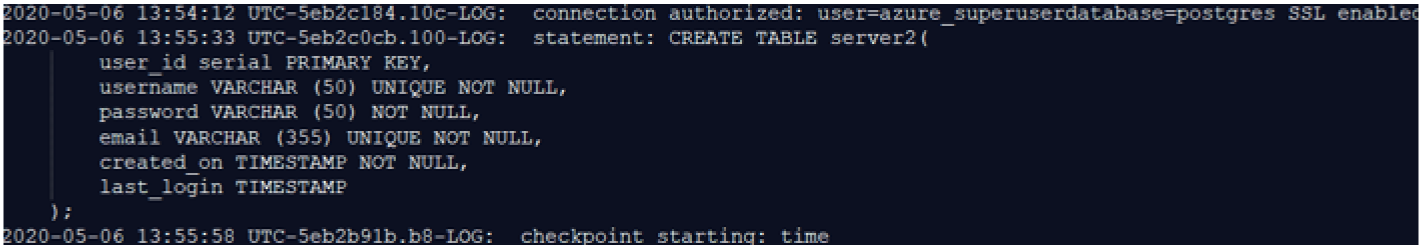
TimeGenerated	2020-05-06T13:55:20
LogicalServerName_s	pg182us
Message	statement: CREATE TABLE server1(user_id serial PRIMARY KEY, username VARCHAR (50) UNIQUE NOT NULL, password VARCHAR (50) NOT NULL, email VARCHAR (355) UNIQUE NOT NULL, created_on TIMESTAMP NOT NULL, last_login TIMESTAMP);
TimeGenerated	2020-05-06T14:21:45
LogicalServerName_s	pg182v2
Message	statement: CREATE TABLE server1(user_id serial PRIMARY KEY, username VARCHAR (50) UNIQUE NOT NULL, password VARCHAR (50) NOT NULL, email VARCHAR (355) UNIQUE NOT NULL, created_on TIMESTAMP NOT NULL, last_login TIMESTAMP);

Now, with the alert setup, you can always correlate with the server logs:



Name	Last update time	Size
postgresql-2020-05-06_131817.log	Wed, 06 May 2020 13:56:06 GMT	15KB

The text file will contain the exact statement (for example, if on the alert email the query text is truncated)



```
2020-05-06 13:54:12 UTC-5eb2c184.10c-LOG:  connection authorized: user=azure_superuserdatabase=postgres SSL enable
2020-05-06 13:55:33 UTC-5eb2c0cb.100-LOG:  statement: CREATE TABLE server2(
        user_id serial PRIMARY KEY,
        username VARCHAR (50) UNIQUE NOT NULL,
        password VARCHAR (50) NOT NULL,
        email VARCHAR (355) UNIQUE NOT NULL,
        created_on TIMESTAMP NOT NULL,
        last_login TIMESTAMP
    );
2020-05-06 13:55:58 UTC-5eb2b91b.b8-LOG:  checkpoint starting: time
```

How good have you found this content?

🙂 🙁