Function App Connectors Kusto Queries

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Contents

Troubleshooting Steps

Function App connectors are using API requests to ingest data into Log Analytics. These request usually involve a "Get" request on the source of the data and a "Post" request to the Workspace Endpoint

Checking ARM requests:

Outgoing

```
cluster("ARMprod.kusto.windows.net").database("ARMProd").HttpOutgoingRequests
| where TIMESTAMP > ago(5d)
| where subscriptionId contains "38b0d074-93c5-40df-b6ae-7400b4b52804"
| where httpMethod contains "get"
```

Incoming

```
cluster("ARMprod.kusto.windows.net").database("ARMProd").HttpIncomingRequests
| where TIMESTAMP > ago(1d)
| where subscriptionId == "38b0d074-93c5-40df-b6ae-7400b4b52804"//
//| where httpStatusCode !in ("200")
//| where * contains "?api-version=2016-04-01"
| where operationName contains "Microsoft.Operationalinsights" or operationName contains "microsoft.securityin
```

Note: Post requests to the Workspace are not visible in ARM, however any request to the Sentinel Endpoint will be seen.

Checking Log Analytics Mem for sign of the logs:

```
cluster('omsgenevatlm.kusto.windows.net').database('OperationInsights_InMem_PROD').ACE
| where TIMESTAMP  between (datetime(2-14-2022) .. 1d)
| where properties  contains "c345088f-2050-4bd2-8d03-c6df2e92f5c9" // Workspace ID
| parse properties with * " DataTypeId=[" datatype "]" *
//| where datatype  contains "SentinelOne_API" //Example of connector application
```

Note: Within the "Message" field the Committed parameter can be seen - "Committed = 0" means that the message has not been ingested into the Workspace

Checking Not Committed Reason

```
cluster('omsgenevatlm.kusto.windows.net').database('OperationInsights_InMem_PROD').AFE
|where TIMESTAMP > ago(30d) and properties contains "b979bac6-3a1f-474d-bc6e-b01388d907fa" and properties cont
```

Note: An example of an error can be that the Custom Fields of the logs are > 500 which is the current limitation from LA. Log Analytics has deprecated the option of expanding the column number of custom logs on specific Workspaces

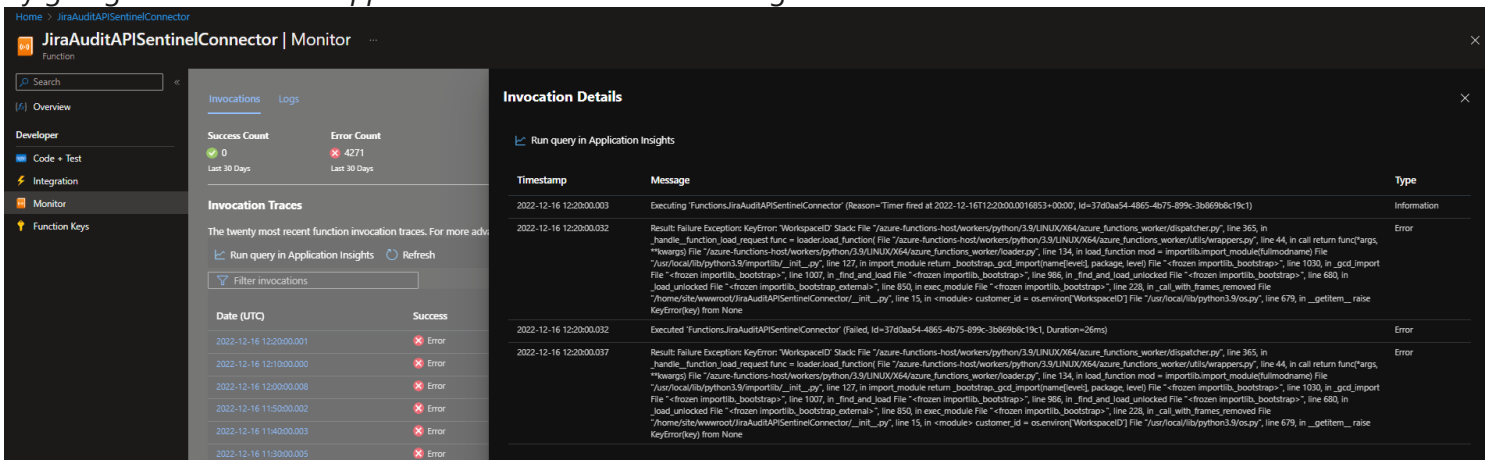
If the issue is the column number and the Function App is created by MS, the issue will have to be raised to our PG to change the FA.

Detailed runtime debugs logs

Further details might be also present in the debug logs when the Function App run. To see them there are two ways.

Customer point of view

By going in the *Function App -> Monitor* and then selecting an execution to see the details.



Azure Support Center

Once we know the Function App name we can try and search for the same logs in *Microsoft.Insights -> components -> <FunctionAppName>* using the following query (taken from *Run query in Application Insights* from the previous screenshot):

```
union traces
| union exceptions
| where timestamp > ago(30d)
//| where operation_Id == '36864dc4b3248e8e97fb0c3d699cd82e'
//| where customDimensions['InvocationId'] == '37d0aa54-4865-4b75-899c-3b869b8c19c1'
| order by timestamp desc
| project timestamp, message = iff(message != '', message, iff(innermostMessage != '', innermostMessage, custo
```