

Function App Connectors Kusto Queries

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

Contents

- [Troubleshooting Steps](#)
 - [Checking ARM requests:](#)
 - [Checking Log Analytics Mem for sign of the logs:](#)
 - [Checking Not Committed Reason](#)
- [Detailed runtime debugs logs](#)
 - [Customer point of view](#)
 - [Azure Support Center](#)

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.

Home

JiraAuditAPISentinelConnector

JiraAuditAPISentinelConnector | Monitor

Function

Search

Overview

Developer

Code + Test

Integration

Monitor

Function Keys

Invocations

Logs

Success Count

0

Last 30 Days

Error Count

4271

Last 30 Days

Invocation Traces

The twenty most recent function invocation traces. For more adv

Run query in Application Insights

Refresh

Filter invocations

Date (UTC)	Success
2022-12-16 12:20:00.001	Error
2022-12-16 12:12:00.000	Error
2022-12-16 12:00:00.008	Error
2022-12-16 11:50:00.002	Error
2022-12-16 11:40:00.003	Error
2022-12-16 11:30:00.004	Error

Invocation Details

Run query in Application Insights

Timestamp	Message	Type
2022-12-16 12:20:00.003	Executing Functions.JiraAuditAPISentinelConnector (Reason=Timer fired at 2022-12-16T12:20:00.0016853+00:00, Id=37d0a54-4865-4b75-899c-3b689b0c19c1)	Information
2022-12-16 12:20:00.032	Result: Failure Exceptions:KeyError: 'WorkspaceId' Stack: File "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/dispatcher.py", line 365, in handle_function_load_request func = loader.load_function(file "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/utils/wrappers.py", line 44, in call return func(*args, **kwargs) File "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/loader.py", line 134, in load_function mod = importlib.import_module(fullmodule_name) File "azur/local/lib/python3.9/importlib__init__.py", line 127, in import_module return _bootstrap._gcd_import(name[level], package, level) File "frozen importlib__bootstrap__", line 1030, in _gcd_import File "frozen importlib__bootstrap__", line 1007, in _find_and_load File "frozen importlib__bootstrap__", line 986, in _find_and_load_unlocked File "frozen importlib__bootstrap__", line 680, in _load_unlocked File "frozen importlib__bootstrap_external__", line 850, in exec_module File "frozen importlib__bootstrap__", line 228, in _call_with_frames_removed File "home/site/wwwroot/JiraAuditAPISentinelConnector__init__.py", line 15, in <module> customer_id = os.environ['WorkspaceId'] File "usr/local/lib/python3.9/os.py", line 679, in __getitem__ raise KeyError(key) from None	Error
2022-12-16 12:20:00.032	Executed Functions.JiraAuditAPISentinelConnector (Failed, Id=37d0a54-4865-4b75-899c-3b689b0c19c1, Duration=26ms)	Error
2022-12-16 12:20:00.037	Result: Failure Exceptions:KeyError: 'WorkspaceId' Stack: File "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/dispatcher.py", line 365, in handle_function_load_request func = loader.load_function(file "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/utils/wrappers.py", line 44, in call return func(*args, **kwargs) File "azure-functions-host/workers/python/3.9/INUX/X64/azure_functions_worker/loader.py", line 134, in load_function mod = importlib.import_module(fullmodule_name) File "azur/local/lib/python3.9/importlib__init__.py", line 127, in import_module return _bootstrap._gcd_import(name[level], package, level) File "frozen importlib__bootstrap__", line 1030, in _gcd_import File "frozen importlib__bootstrap__", line 1007, in _find_and_load File "frozen importlib__bootstrap__", line 986, in _find_and_load_unlocked File "frozen importlib__bootstrap__", line 680, in _load_unlocked File "frozen importlib__bootstrap_external__", line 850, in exec_module File "frozen importlib__bootstrap__", line 228, in _call_with_frames_removed File "home/site/wwwroot/JiraAuditAPISentinelConnector__init__.py", line 15, in <module> customer_id = os.environ['WorkspaceId'] File "usr/local/lib/python3.9/os.py", line 679, in __getitem__ raise KeyError(key) from None	Error

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
```

Case # [REDACTED] for d****[REDACTED]

[View case details](#)[Escalate case](#)

Subscriptions

Quick access

No items in quick access yet.

+ Add subscription

Resource provider

Search for resources

X

Completed loading live data for subscription 9847c31e-e02e-475c-9252-d13576c0558d

Show additional status

microsoft.alertsmanagement

Microsoft Insights

actiongroups

components

Resource Change HistoryAccess ControlAzure Monitor MetricsHealth

Kusto query tabRecommendation

Kusto query tab

Log Analytics Wiki and Common queries

Kusto Query

union traces
| union exceptions
| where timestamp > ago(30d)
//| where operation_Id == '36864dc4b3248e8e97fb0c3d699cd82e'

Time Range

Last 24 Hours

Custom Start Time

Select date time...

Custom End Time

Select date time...

Run

Drag a column header and drop it here to group by that column

timestamp	message	logLevel
+ 12/15/2022 12:23:24 PM	INFORMATION: APIStatusCode:401 APIStatusMessage:Microsoft.PowerShell.Commands.HttpResponseException: Response status code does not indicate success: 401 (Unauthorized), at System.Management.Automation.MshCommandRuntime.ThrowTerminatingError(ErrorRecord errorRecord).Message: Error @ line #284. I'm exiting!	Information