

# Check the memory usage for scanning

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:10 PM PST

## Purpose

For Scanning, we can check the memory usage of the **customer machine** from logs directly.

## To check the used memory percentage:

```
cluster("https://azuredmprod.kusto.windows.net").database("AzureDataMovement").
TraceGatewayLocalEventLog
| where UserReportId == "cab6ed66-eeeb-4f09-8b80-80cfa1253ddd"
| where LocalMessage contains "eventId: ExecutionDataScanActivity"
| where LocalMessage contains "Used memory percentage is"
| project LocalMessage
```

For miti: If the used memory percentage is too high like 98%-99%, which cannot guarantee the proper behavior of scanning.

For non-miti: If the used memory percentage is 70%, one of agent processes will try to quit. If the used memory percentage is 90%, executor will force kill one of agent processes. Both operations here are from code, which are trying to auto reduce memory.

## To check the memory usage for all processes:

```
cluster("https://azuredmprod.kusto.windows.net").database("AzureDataMovement").
TraceGatewayLocalEventLog
| where UserReportId == "cab6ed66-eeeb-4f09-8b80-80cfa1253ddd"
| where LocalMessage contains "eventId: ExecutionDataScanActivity"
| where LocalMessage contains "MemUsage"
| project LocalMessage
```

The result will be like below - you can write a script to check it in excel.

LocalMessage
PrimaryResult  Query Summary  QueryStatus  Issues: (2)
LocalMessage
eventId: ExecutionDataScanActivity
message: MemUsage: 171696128/8588906496 9812:348:2854912:101:cmd 3544:-1:1744896:148:vm3dservice 6892:-1:1712128:178:svchost 1768:-1:1892352:173:svchost 6692:-1:20258816:317:svchost 2356:4656:107708416:1035:diawp 8068:-1:3432448:218:RuntimeBroker 1960:-1:1314816:170:svchost 684:-1:3190784:215:svchost 3140:-1:9007104:591:spoolsv 1168:-1:1675264:48:fontdrvhost 10152:2356:43180032:618:Microsoft.DataMap.Agent 772:-1:11051008:1654:lsass 968:-1:2244608:230:winlogon 3528:-1:11227136:414:vmtoolsd 4656:4760:117923840:1462:diahost 768:-1:8183808:292:svchost 1160:-1:1548288:48:fontdrvhost 10024:4656:89337856:711:diawp 4760:700:19578880:320:dmqsvc 3428:4656:89272320:711:diawp 3520:-1:4431872:230:taskhostw 1352:-1:13135872:474:LogonUI 3912:-1:2830336:330:rdpclip

### Example and the meaning for each number:

MemUsage: 171696128/8588906496 9812:348:2854912:101:cmd | | Available Memory | Total Memory | ProcessId | ParentId | memory | |ProcessName | |--|--|--|--  
|--|--|--|-- | MemUsage: |171696128 |8588906496| 9812| 348 | 2854912 | 101 |cmd |

### Some known processes:

- diawp -> Executor process
- Microsoft.DataMap.Agent -> Agent process

### Tips:

To check if a process is created for scanning: follow the processId->parentId pattern to find if it's related to our known processes.