NIC Cloud Connect

Oslo Spektrum

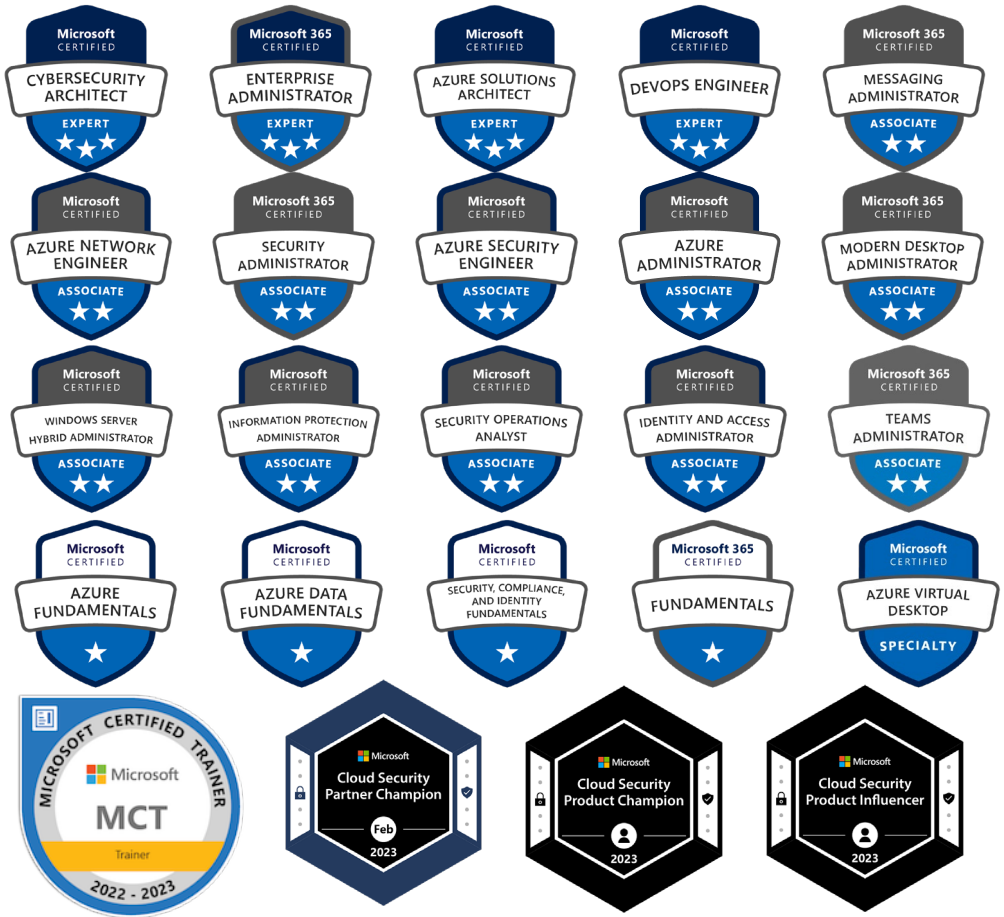
November 7 - 9

NIC Cloud Connect

Morten Knudsen

Unleash the Power of Azure Resource Graph

Speaker – Morten Knudsen



About | Morten Knudsen

Microsoft MVP Security & Azure Hybrid MVP

Microsoft Certified Trainer

Cloud & Security Architect

Microsoft Sentinel Black Belt

Microsoft Defender Black Belt

Microsoft Cloud Security Influencer

Microsoft Sentinel Influencer

Microsoft Defender for Cloud Influencer

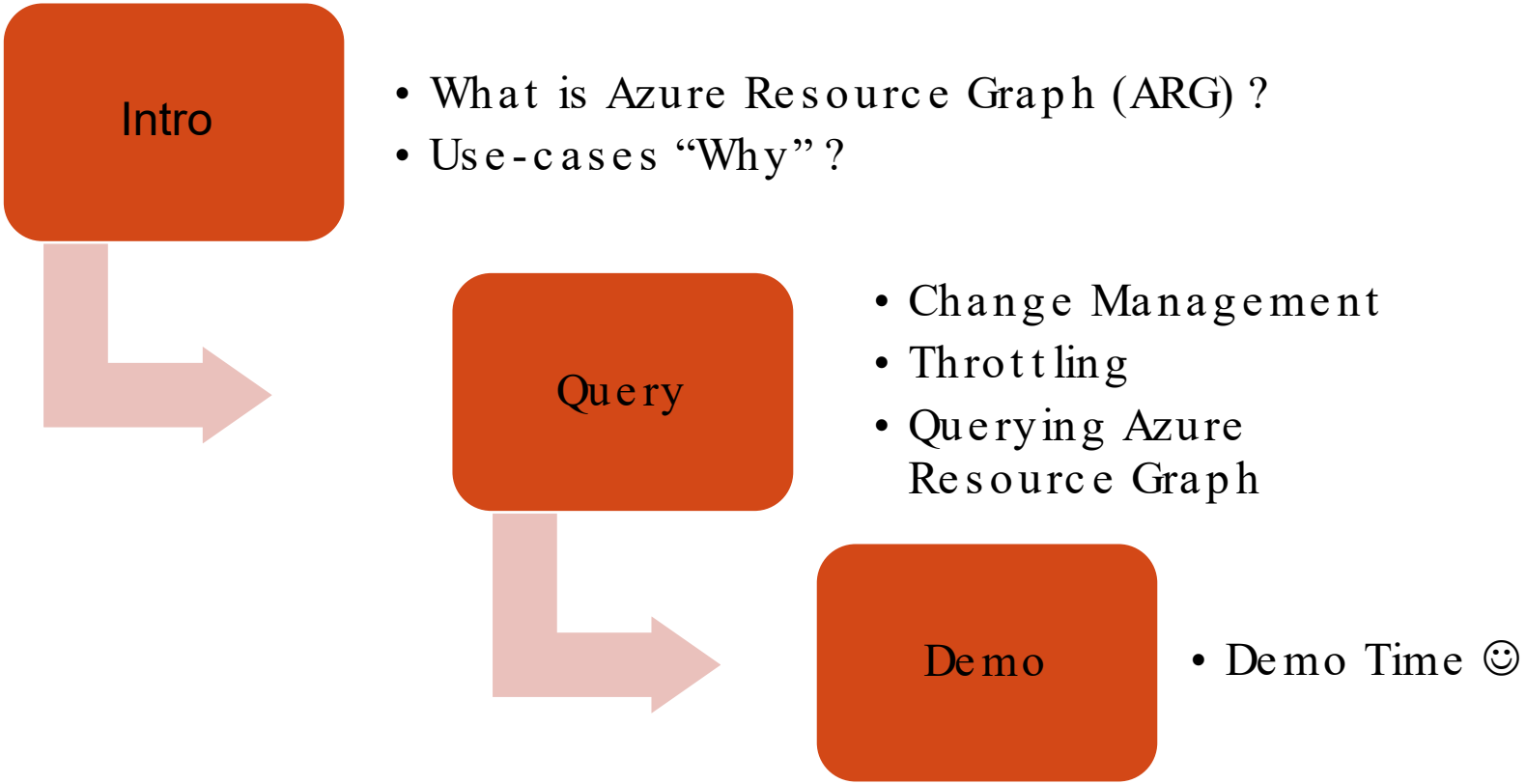
MVP Microsoft® Most Valuable Professional

Award Categories
Security

First year awarded:
2023

Number of MVP Awards:
1

Agenda


Intro
• What is Azure Resource Graph (ARG) ?
• Use-cases “Why” ?
Query
• Change Management
• Throttling
• Querying Azure Resource Graph
Demo
• Demo Time ☺

This presentation

Struggles without an index

- Performance would be very SLOW !!
  - Traverse each resource to get all properties
    - Get a list of all storage account with public access ?
    - Get a list of all VMs with Tag Environment = Prod ?
    - Get me a list of RBACs where x is delegated?

- Cost would be high
  - If we had to build our own indexes using script
    - Lots of data

What is Azure Resource Graph (ARG) ?

Index with All properties from Azure Resource Providers (Resources, Policies, Security and more)

Query at scale (very fast!)

Distributed index store. Data is partitioned into disjoint sets across different machines and queries are executed across those partitions in parallel

Kusto Query Language (KQL)

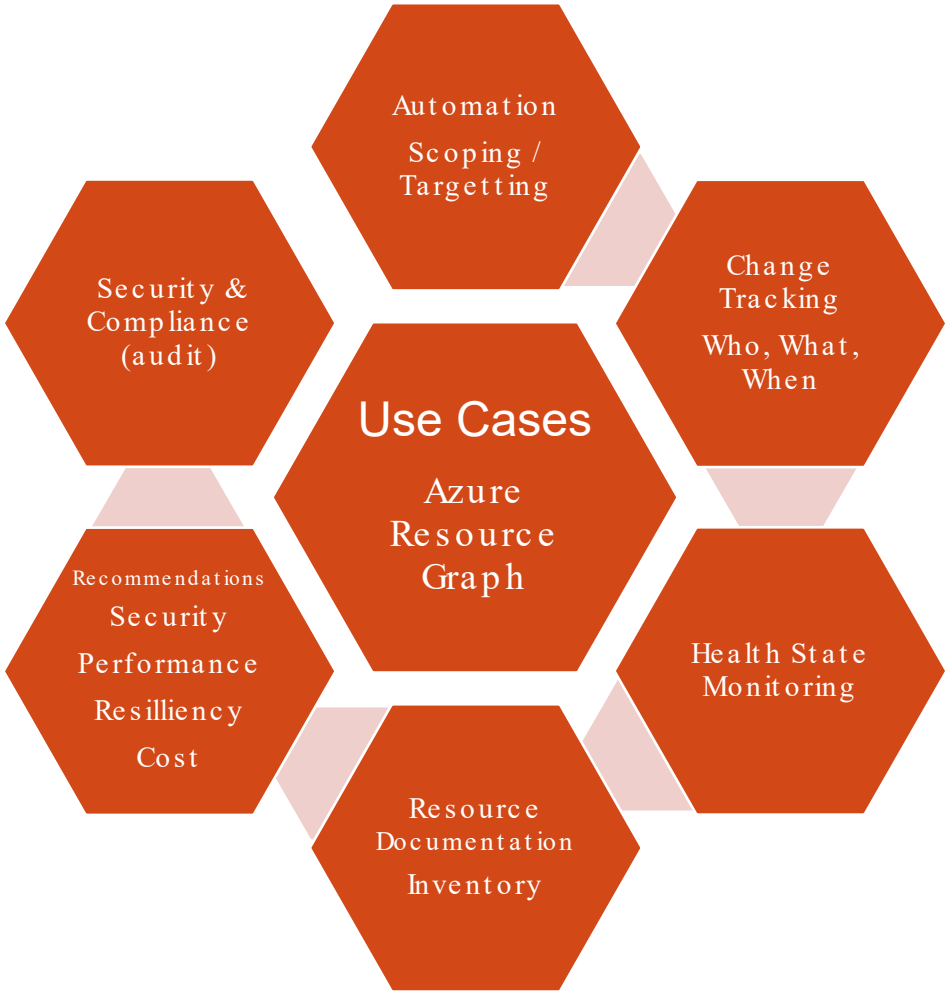
Kusto Platform

(optimized for inventory scenarios)

Read Permission in Azure RBAC is required

Support for Azure Lighthouse

THE WHY !


Automation
Scoping / Targetting
Change Tracking
Who, What, When
Security & Compliance (audit)
Use Cases
Azure Resource Graph
Recommendations
Security
Performance
Resilliency
Cost
Health State Monitoring
Resource Documentation
Inventory

How is Azure Resource Graph kept current ?

Creates, Updated and deletes makes Change Records

New change resource (Microsoft.Resources/changes) is created to extend the modified resource and represent the changed properties

Change records should be **available in less than five minutes**

Full Scan daily - Missed notifications or when a resource is updated outside of Resource Manager.


```
"targetResourceId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/myResourceGroup/providers/microsoft.compute/virtualmachines/myVM",
 "targetResourceType": "microsoft.compute/virtualmachines",
 "changeType": "Update",
 "changeAttributes": {
  "changesCount": 2,
  "correlationId": "88420d5d-8d0e-471f-9115-10d34750c617",
  "timestamp": "2021-12-07T09:25:41.756Z",
  "previousResourceSnapshotId": "ed90e35a-1661-42cc-a44c-e27f508005be",
  "newResourceSnapshotId": "6eac9d0f-63b4-4e7f-97a5-740c73757efb"
 },
 "changes": {
  "properties.provisioningState": {
   "newValue": "Succeeded",
   "previousValue": "Updating",
   "changeCategory": "System",
   "propertyChangeType": "Update"
   "isTruncated":"true"
  },
  "tags.key1": {
   "newValue": "NewTagValue",
   "previousValue": "null",
   "changeCategory": "User",
   "propertyChangeType": "Insert"
```

New query | Open a query | Set authorization scope | Run query | Save | Save as | Feedback

Query 1 | Query 3 | Query 4 | Query 5 | Query 6

```
1  resourcechanges
2  | project properties.changeAttributes.timestamp, properties.changeType, properties.targetResourceId, properties.targetResourceType, properties.changes
3  | limit 5
4
5
```

Get started | Results | Charts | Messages

Download as CSV | Pin to dashboard | Formatte

properties_changeAttributes_timest...	properties_changeType	properties_targetResourceId	properties_targetResourceType	properties_changes	
2023-08-10T03:04:29.7450000Z	Update	/subscriptions/fce4f282-fcc6-43fb-94d...	microsoft.compute/virtualmachines/ext...	{"properties.provisioningState":{"proper...	See details
2023-08-12T04:43:09.8270513Z	Update	/subscriptions/fce4f282-fcc6-43fb-94d...	microsoft.network/virtualnetworks	{"properties.subnets[1].properties.ipCo...	See details
2023-08-12T04:43:14.0550357Z	Update	/subscriptions/fce4f282-fcc6-43fb-94d...	microsoft.network/networkinterfaces	{"properties.ipConfigurations[0].proper...	See details
2023-08-12T04:43:03.6317612Z	Update	/subscriptions/fce4f282-fcc6-43fb-94d...	microsoft.network/networksecuritygrou...	{"properties.networkInterfaces[0].id":{"p...	See details
2023-08-03T10:43:07.8414926Z	Update	/subscriptions/fce4f282-fcc6-43fb-94d...	microsoft.web/connections	{"properties.api.iconUri":{"propertyCha...	See details

Throttling

TIP: make 5 sec delay between queries

Azure Resource Graph is a free service

Provide the best experience and response time for all customers

Large-scale and frequent queries – Support -ticket MS (business case)

Resource Graph throttles queries at the user level (context)

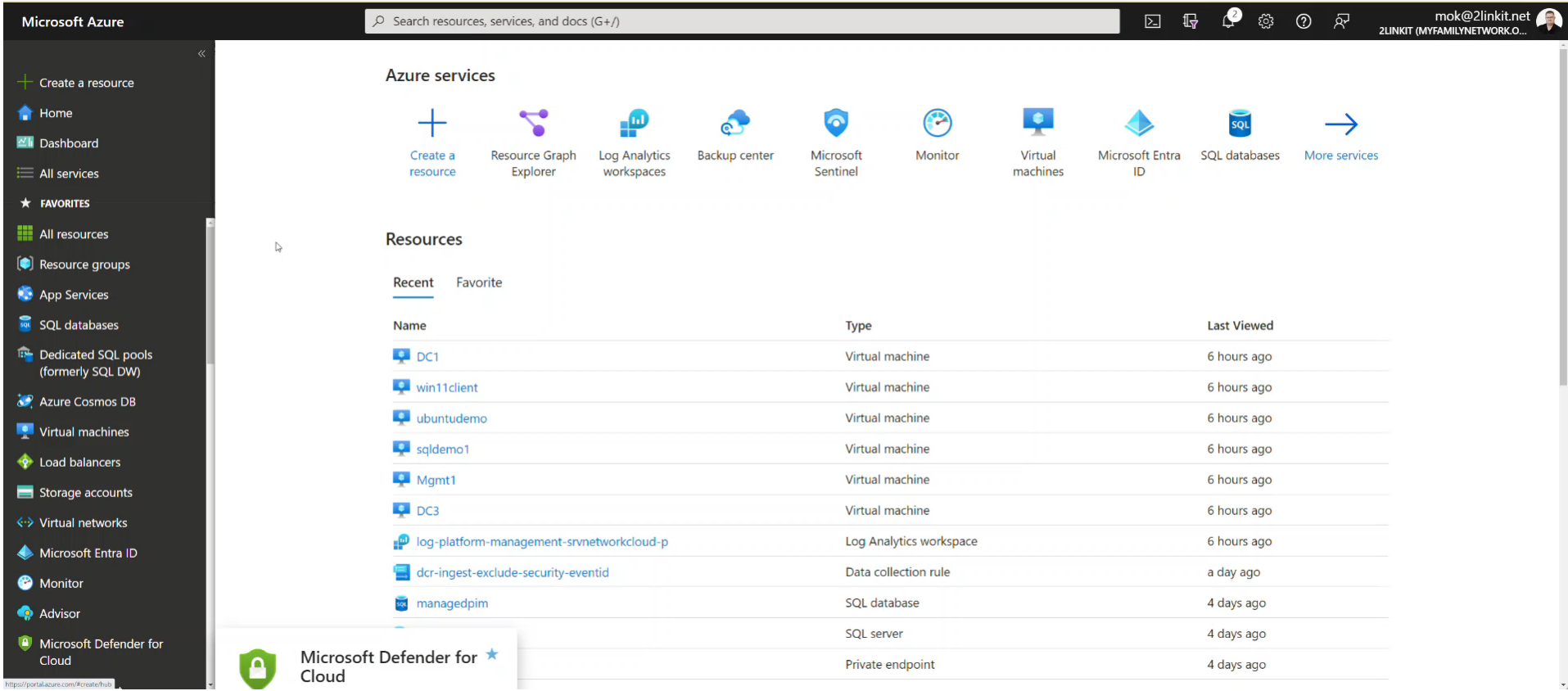
nic Cloud Connect

Running your first query using Kusto against ARG

11 methods

- Azure Portal
- Azure CLI
- Azure Powershell (Search -AzGraph)
- Query using AzResourceGraphPS
- .NET
- Go
- Java
- JavaScript
- Python
- Ruby
- REST API

Query using Azure Portal (02:27)



Azure CLI

- **az graph query** –q “<query>”

- **az graph query** -q "alertsmanagementresources | where properties.essentials.startDateTime > ago(12h) | project alertId = id, name, monitorCondition = tostring (properties.essentials.monitorCondition), severity = tostring (properties.essentials.severity), monitorService = tostring (properties.essentials.monitorService), alertState = tostring (properties.essentials.alertState), targetResourceType = tostring (properties.essentials.targetResourceType), targetResource = tostring (properties.essentials.targetResource), subscriptionId, startDateTime = todatetime (properties.essentials.startDateTime), lastModifiedDateTime = todatetime (properties.essentials.lastModifiedDateTime), dimensions = properties.context.context.condition.allOf [0].dimensions, properties"

Administrator: Windows PowerShell

```
PS C:\Windows\system32> az login --tenant "f0fa27a0-8e7c-4f63-9a77-ec94786b7c9e"
```

Powershell

Search-AzGraph

(Az.ResourceGraph)

```
1  $Query = @"
2  resourcecontainers
3  | where type == 'microsoft.management/managementgroups'
4  | extend mgParent = properties.details.managementGroupAncestorsChain
5  | mv-expand with_itemindex=MGHierarchy mgParent
6  | project id, name, properties.displayName, mgParent, MGHierarchy, mgParent.name
7  | sort by MGHierarchy asc
8  "@
9
10
11 Search-AzGraph -Query $Query -UseTenantScope
12
```

```
MGHierarchy             : 2
mgParent_name           : f0fa27a0-8e7c-4f63-9a77-ec94786b7c9e
ResourceId              : /providers/Microsoft.Management/managementGroups/mg-sandboxes-corp

id                      : /providers/Microsoft.Management/managementGroups/mg-sandboxes-corp-
                          policytesting
name                    : mg-sandboxes-corp-policytesting
properties_displayName  : Sandboxes_Corp_PolicyTestting
mgParent                : @{displayName=2LINKIT; name=mg-2linkit}
MGHierarchy             : 2
mgParent_name           : mg-2linkit
ResourceId              : /providers/Microsoft.Management/managementGroups/mg-sandboxes-corp-
                          policytesting

id                      : /providers/Microsoft.Management/managementGroups/mg-sandboxes-onlin
                          e
name                    : mg-sandboxes-online
properties_displayName  : Sandboxes_Online
mgParent                : @{displayName=Tenant Root Group; name=f0fa27a0-8e7c-4f63-9a77-ec947
                          86b7c9e}
MGHierarchy             : 2
mgParent_name           : f0fa27a0-8e7c-4f63-9a77-ec94786b7c9e
ResourceId              : /providers/Microsoft.Management/managementGroups/mg-sandboxes-onlin
                          e
```

Search - AzGraph (01:48)

```powershell
#-------------------------------------------------------
# Get Azure Policy Assignments
#-------------------------------------------------------
    Write-Output "Getting Policy Assignments from Azure Resource Graph using TenantScope"
    $AzPolicyAssignments = @()

    $pageSize = 1000
    $iteration = 0
    $searchParams = @{
                        Query = "policyresources `
                                 | where type == 'microsoft.authorization/policyassignments' "
                        First = $pageSize
                    }

    $results = do {
        $iteration += 1
        $pageResults = Search-AzGraph  @searchParams -UseTenantScope
        $searchParams.Skip += $pageResults.Count
        $AzPolicyAssignments += $pageResults
    } while ($pageResults.Count -eq $pageSize)


#
```

```
id              : /providers/Microsoft.Management/managementGroups/mg-Infrastructure-Simple/providers/Microsoft.Authorization/policyAs
                  signments/DiagTablesLAWS_IAC
name            : DiagTablesLAWS_IAC
type            : microsoft.authorization/policyassignments
tenantId        : f0fa27a0-8e7c-4f63-9a77-ec94786b7c9e
kind            : policyassignments
location        : westeurope
```

GiveAway Questions 1&2

What query language is used to retrieve data from Azure Resource Graph ?

How many methods exist to retrieve ARG data incl. my PS module?

Come up to me afterwards ☺

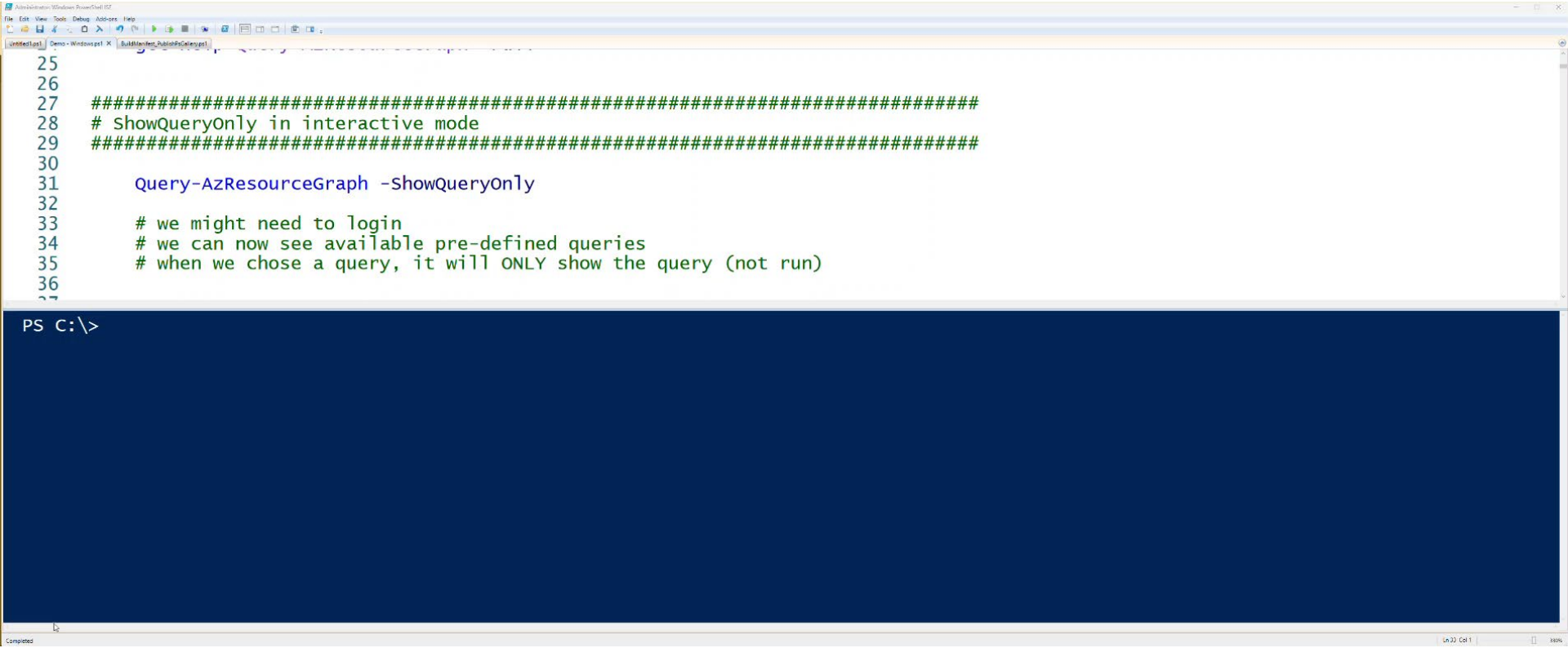
AzResourceGraphPS by Morten Knudsen

Community / Free
Available on PowerShell Gallery

- Query against Tenant, MG, Sub
- Run Query or ShowQueryOnly -mode
- Query using +100 pre-defined queries
- Commandline and Interactive -mode
- Run Custom Queries
- Query with Azure App/Secret
- Filtering: Skip, First
- Automatic update existing queries & get new queries

Think of it as a wrapper – the real power is ARG ☺

Deep-dive into AzResourceGraphPS on Windows (06:45)



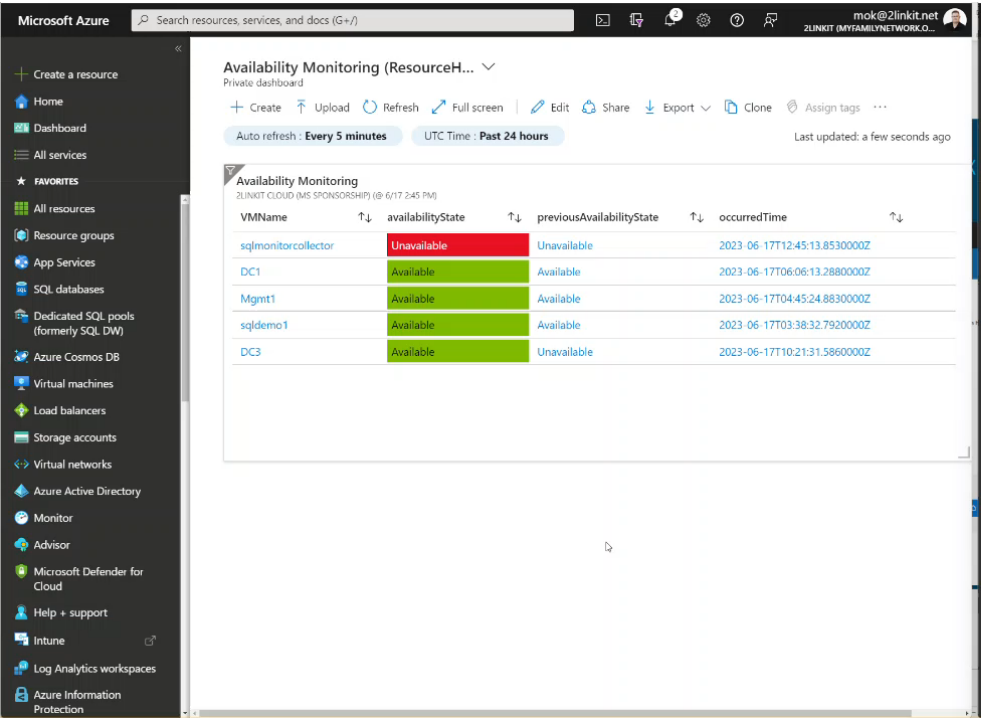
Sample use-cases of data from Azure Resource Graph (07:27)

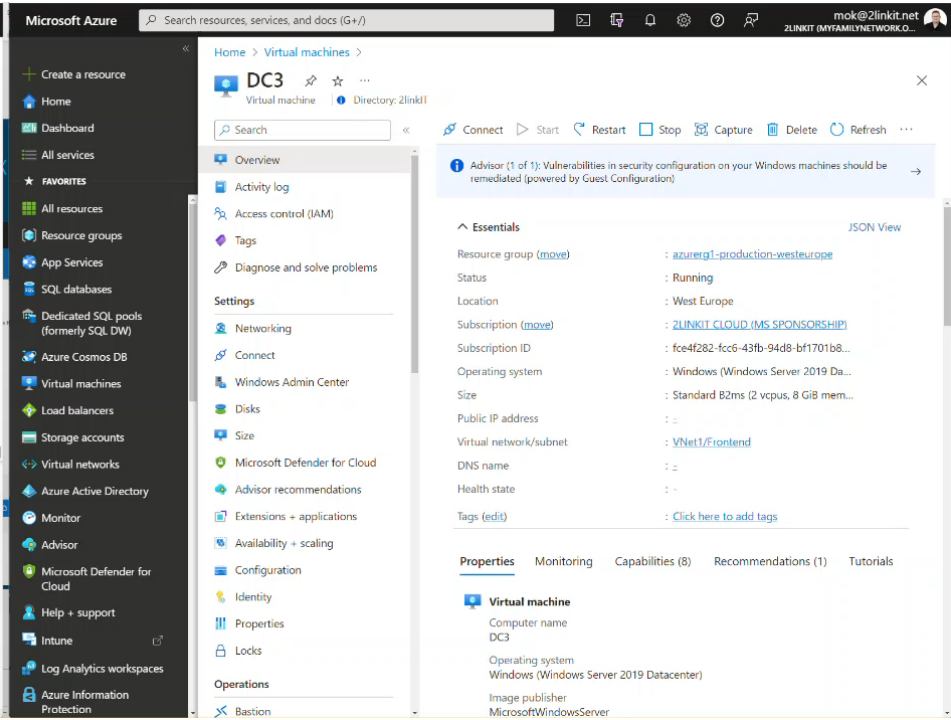
```
562
563  ##############################################################################################
564  # Inspiration | Examples of use cases of data from Azure Resource Graph
565  # Data can be used as part of Reports, Alerts, Dashboards, Workbooks
566  ##############################################################################################
567
568  # Get Orphaned Disks
569  AzOrphanedDisks-Query-AzARG | Query-AzResourceGraph -QueryScope "Tenant" -AzAppId $AzAppId -AzAppSecret $AzAppSecret -TenantId $TenantId
570
571  #------------------------------
572
```

```
------------------------------------------------------------------------

Running Query against Azure Resource Graph ... Please Wait !

Raw Records Received (excluding header record):
3

Time Used to Get Records:
00:00:00.4494888


VMName availabilityState previousAvailabilityState occurredTime        subscriptionName               subscriptionId
------ ----------------- ------------------------- ------------        ----------------               --------------
DC1    Available         Available                 07-10-2023 11:20:19 2LINKIT CLOUD (MS SPONSORSHIP) fce4f282-fcc6-43fb-94d8-bf1701b862c3
Mgmt1  Available         Available                 07-10-2023 11:22:46 2LINKIT CLOUD (MS SPONSORSHIP) fce4f282-fcc6-43fb-94d8-bf1701b862c3
DC3    Unavailable       Unavailable               07-10-2023 16:11:09 2LINKIT CLOUD (MS SPONSORSHIP) fce4f282-fcc6-43fb-94d8-bf1701b862c3



PS C:\>
```

Health State Monitoring using Azure Resource Graph

(02:26)





nic Cloud Connect

Azure Resource Graph Query

```
healthresources
| where type == "microsoft.resourcehealth/availabilitystatuses"
| extend RessId = properties.targetResourceId
| extend previousAvailabilityState = properties.previousAvailabilityState
| extend occurredTime = properties.occurredTime
| extend availabilityState = properties.availabilityState
| extend VMName = split(RessId, "/")[-1]
| sort by tostring(availabilityState) desc
| project VMName, availabilityState, previousAvailabilityState, occurredTime
```

Run AzResourceGraphPS on Ubuntu using Powershell

(0 1:11)

Azure LogAnalytics integration against Azure Resource Graph

```
1  InsightsMetrics
2  | where Name == "UtilizationPercentage"
3  | summarize TimeGenerated = arg_max(TimeGenerated,*) by Computer
4  | lookup (
5      arg("").Resources
6          | where type == 'microsoft.compute/virtualmachines'
7          | project _ResourceId=tolower(id), tags
8      ) on _ResourceId
9  | where tostring(tags.Environment) == "PROD"
10 | project Computer, ProcessorUtilization=round(Val,0)
11 | sort by ProcessorUtilization desc
```

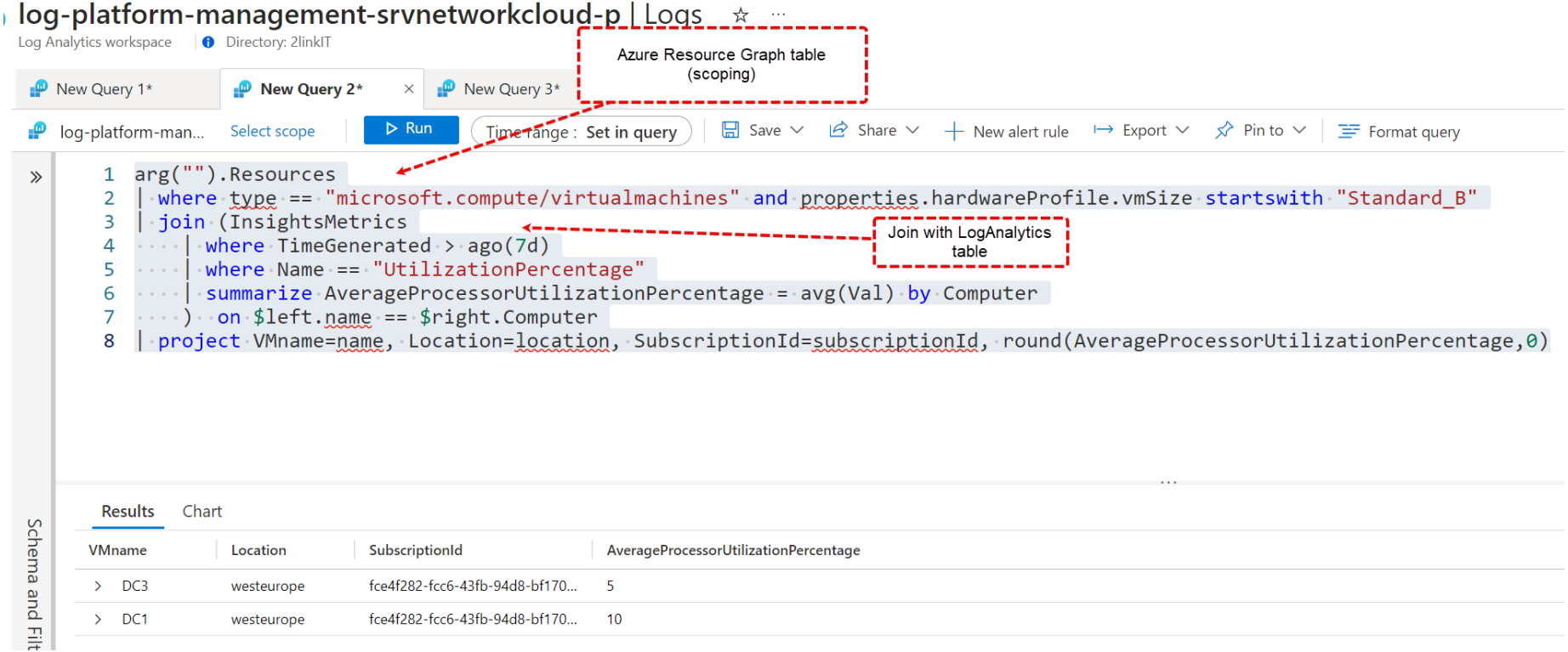
LogAnalytics table

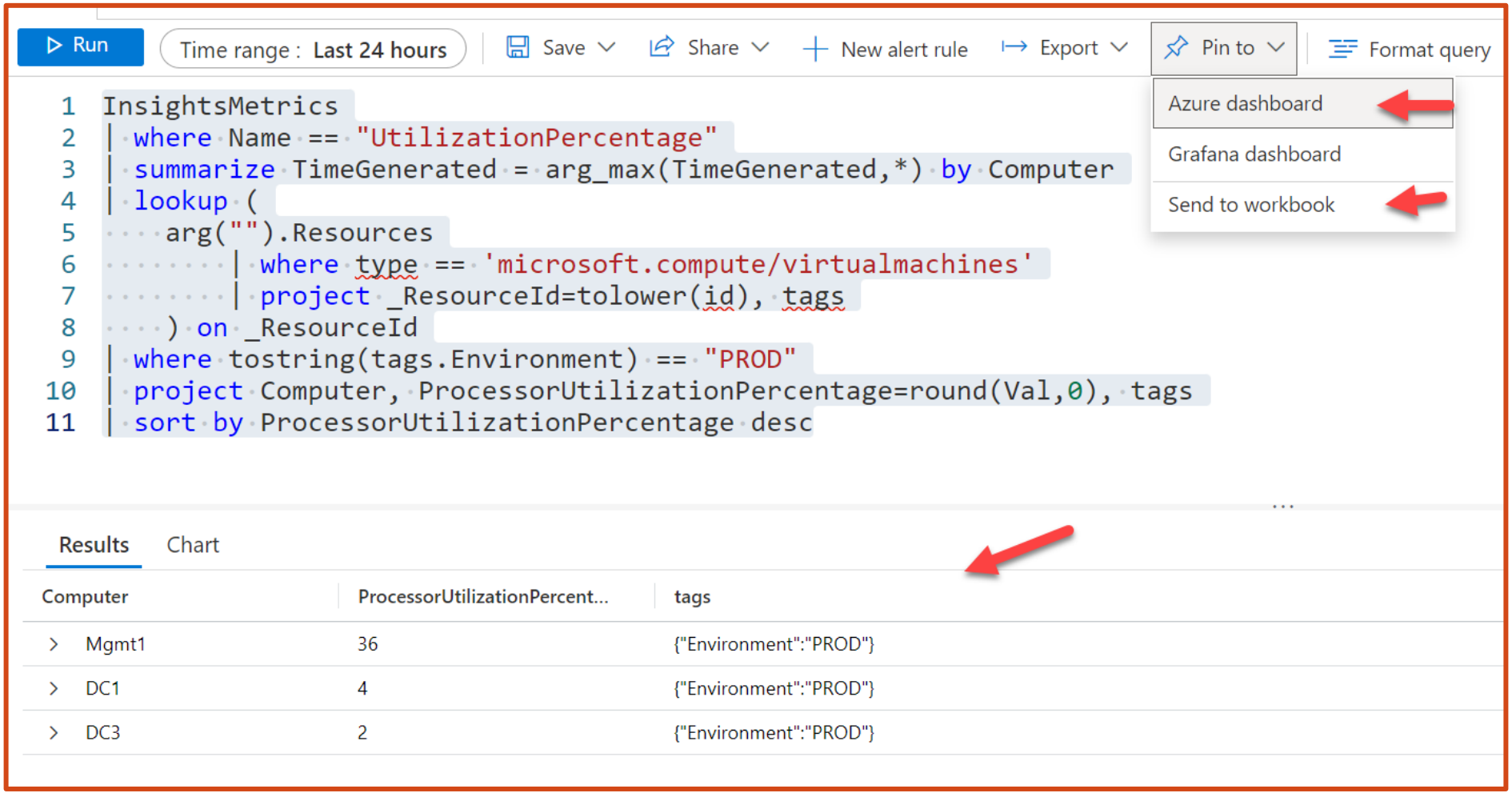
Lookup in ARG table

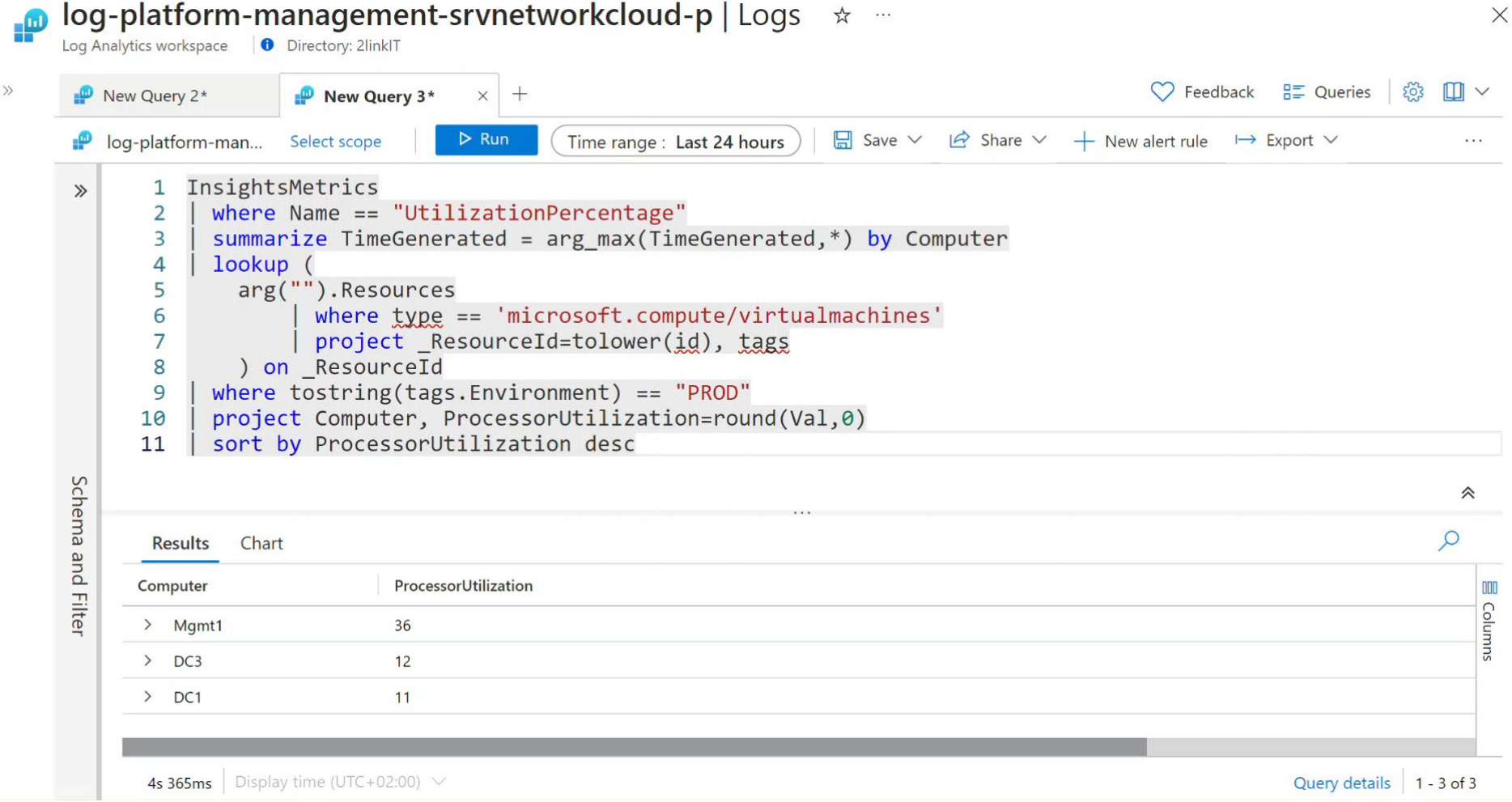
Results | Chart

Computer	ProcessorUtilization
Mgmt1	36
DC3	12
DC1	11

Find all VMs with size Standard_B* and get Average CPU (Last 7 days)




Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Pin to
Format query
Azure dashboard
Grafana dashboard
Send to workbook
InsightsMetrics
| where Name == "UtilizationPercentage"
| summarize TimeGenerated = arg_max(TimeGenerated,*) by Computer
| lookup (
arg("").Resources
| where type == 'microsoft.compute/virtualmachines'
| project _ResourceId=tolower(id), tags
) on _ResourceId
| where tostring(tags.Environment) == "PROD"
| project Computer, ProcessorUtilizationPercentage=round(Val,0), tags
| sort by ProcessorUtilizationPercentage desc
Results
Chart
Computer
ProcessorUtilizationPercent...
tags
Mgmt1
36
{"Environment":"PROD"}
DC1
4
{"Environment":"PROD"}
DC3
2
{"Environment":"PROD"}


log-platform-management-srvnetworkcloud-p | Logs
Log Analytics workspace
Directory: 2linkIT
New Query 2*
New Query 3*
Feedback
Queries
log-platform-man...
Select scope
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
1 InsightsMetrics
2 | where Name == "UtilizationPercentage"
3 | summarize TimeGenerated = arg_max(TimeGenerated,*) by Computer
4 | lookup (
5 arg("").Resources
6 | where type == 'microsoft.compute/virtualmachines'
7 | project _ResourceId=tolower(id), tags
8) on _ResourceId
9 | where tostring(tags.Environment) == "PROD"
10 | project Computer, ProcessorUtilization=round(Val,0)
11 | sort by ProcessorUtilization desc
Schema and Filter
Results
Chart
Computer
ProcessorUtilization
Mgmt1
36
DC3
12
DC1
11
Columns
4s 365ms
Display time (UTC+02:00)
Query details
1 - 3 of 3

Daily Backup Status Mail (01:37)

```powershell
#-------------------------------------------------------------------------------------------------
    Write-Output ""
    Write-Output "Collecting jobs status from RSV vaults .... Please Wait !!"
    $pageSize = 1000
    $searchParams = @{
                    Query = "recoveryservicesresources `
                        | where type == `"microsoft.recoveryservices/vaults/backupjobs`" `
                        | where properties.startTime >= ago(1d) `
                        | where properties.operation != `"ConfigureBackup`" "
                    First = $pageSize
                    }

    $Results = Search-AZGraph @searchParams -ManagementGroup $TenantId
    $RSVVaultJobStatus = $Results

    Write-Output "Bulding statistics for Azure Recovery Vaults .... Please Wait !!"
        If ($RSVVaultJobStatus)
            {
                $RSVCompletedjobs  += $RSVVaultJobStatus | Where-Object({$_.properties.status -eq 'Completed'})
```

```
DataSourceName : 21inkitscriptsbackup
DataSourceType : Microsoft.Storage/storageAccounts/blobServices
Operation      : Backup
PolicyName     : AzStorageBlobDaily
Duration       : 00:18:44.8491553
Status         : Completed
```

Wouldn’t it be cool if …. ☺

- Feedback Meeting with ARG-team in Seattle on Monday Nov 13th
  - PIM – Eligible permissions
  - Health status – ARC machines (+ other resource type)
  - Resource Lifecycle
  - Alerting in ARG (notifications when x happens)
  - Resource Type schema - DCR / LA
  - Bug: version 1.2 (Native VMs) vs. 1.2.3.4 (ARC servers)
  - Logs of query against ARG (audit)

- https://aka.ms/argfeaturerequest

nic Cloud Connect

Get Started with AzResourceGroupPS (Github)

Presentation with demo's

Thank You

Blog: https://mortenknudsen.net

Mail: mok@mortenknudsen.net | mok@2linkit.net

LinkedIn: https://www.linkedin.com/in/mortenwaltorpknudsen

GitHub: https://github.com/KnudsenMorten

X/Twitter: https://twitter.com/knudsenmortendk