



nic Cloud
Connect

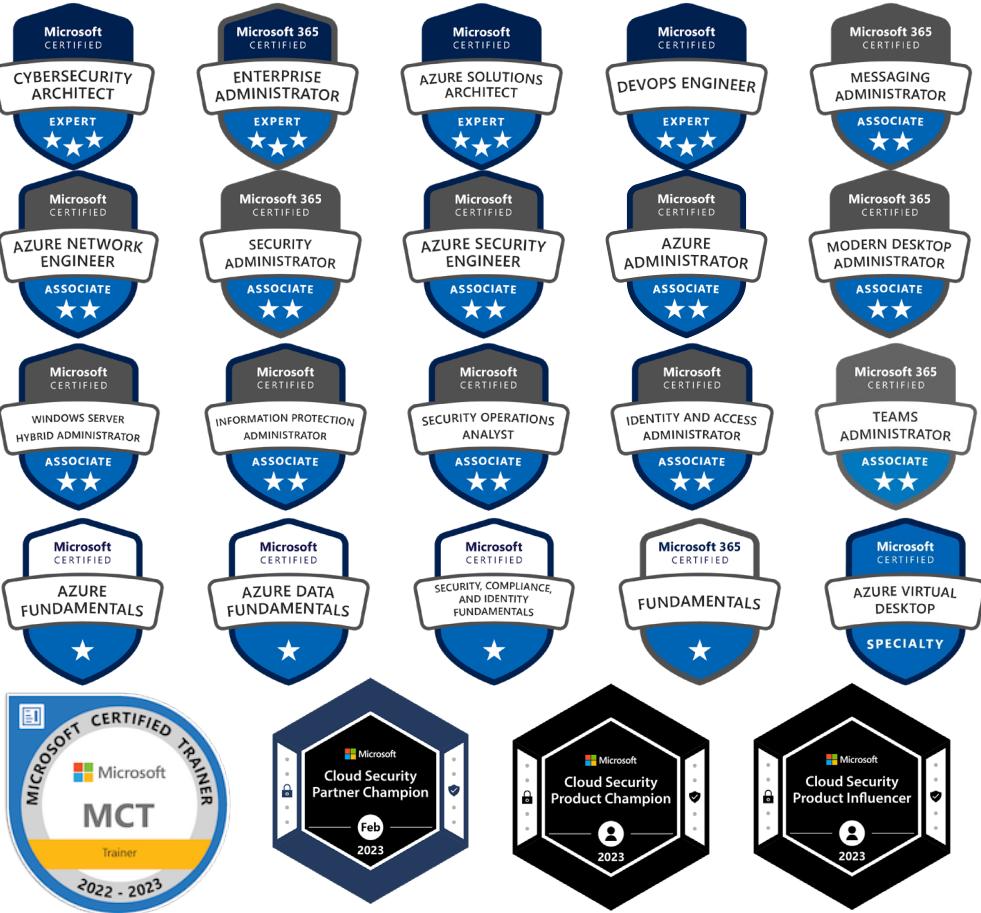
Oslo Spektrum
November 7 - 9



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



Award Categories

Security

First year awarded:

2023

Number of MVP Awards:

1

Agenda

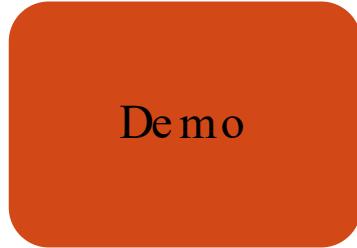
Intro

- 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)

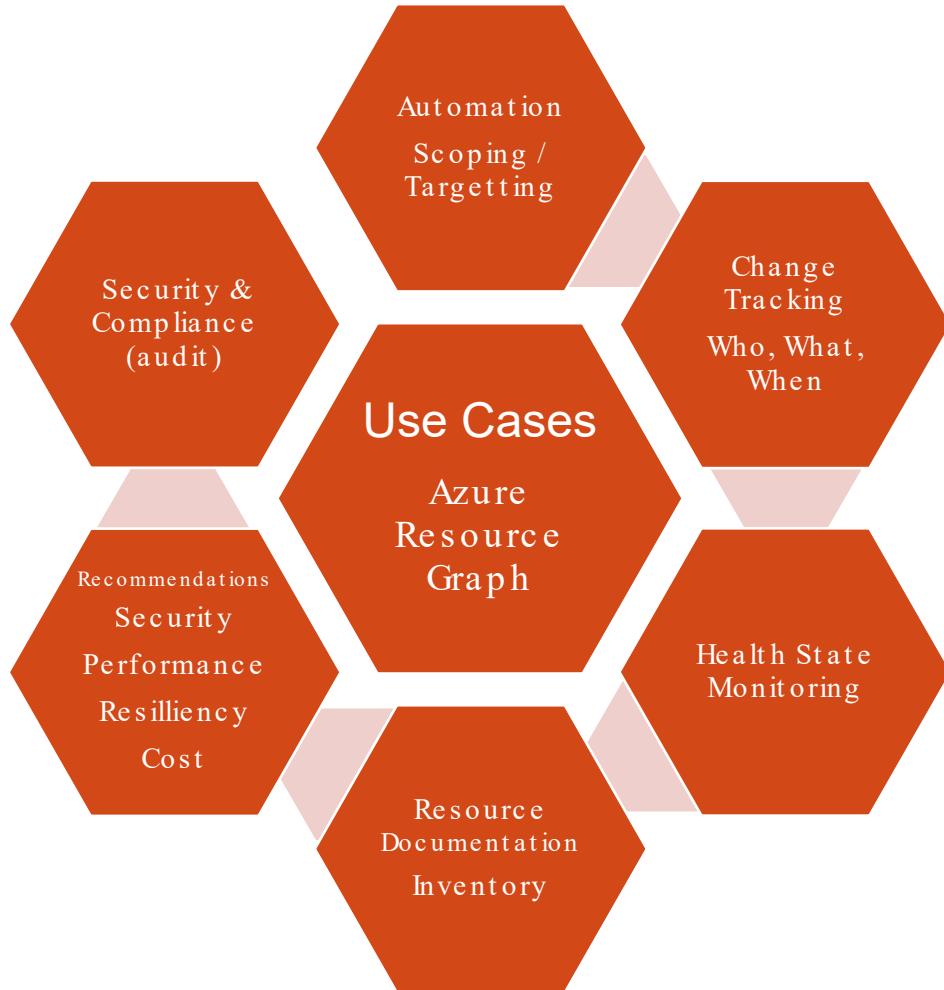


Read Permission in Azure RBAC is required



Support for Azure Lighthouse

THE WHY !



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-a44ce27f508005be",
  "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

Formatter

properties_changeAttributes_timestamp	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)

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)

Microsoft Azure Search resources, services, and docs (G+/-) Logout Help ? Feedback More services mok@2linkit.net 2LINKIT (MYFAMILYNETWORK.O...

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

SQL databases

Dedicated SQL pools (formerly SQL DW)

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Microsoft Entra ID

Monitor

Advisor

Microsoft Defender for Cloud

<https://portal.azure.com/#create/hub>

Azure services

Create a resource Resource Graph Explorer Log Analytics workspaces Backup center Microsoft Sentinel Monitor Virtual machines Microsoft Entra ID SQL databases More services

Resources

Recent Favorite

Name	Type	Last Viewed
DC1	Virtual machine	6 hours ago
win11client	Virtual machine	6 hours ago
ubuntudemo	Virtual machine	6 hours ago
sqldemo1	Virtual machine	6 hours ago
Mgmt1	Virtual machine	6 hours ago
DC3	Virtual machine	6 hours ago
log-platform-management-srvnetworkcloud-p	Log Analytics workspace	6 hours ago
dcr-ingest-exclude-security-eventid	Data collection rule	a day ago
managedpim	SQL database	4 days ago
	SQL server	4 days ago
	Private endpoint	4 days ago

Microsoft Defender for Cloud

Azure CLI

- **az graph query -q "<query>"**
- **az graph query -q "alertsmanagementresources | where properties.essentials.startTime > 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, startTime = todatetime(properties.essentials.startTime), lastModifiedDateTime = todatetime(properties.essentials.lastModifiedDateTime), dimensions = properties.context.context.condition.allOf [0].dimensions, properties"**

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



Powershell

Search - AzGraph
 (Az.ResourceGraph)

```

1 $Query = @"
2 resourcecontainers
| where type == 'microsoft.management/managementgroups'
| extend mgParent = properties.details.managementGroupAncestorschain
| mv-expand with_itemindex=MGHierarchy mgParent
| project id, name, properties.displayName, mgParent, MGHierarchy, mgParent.name
| sort by MGHierarchy asc
"@

2
3
4
5
6
7
8
9
10 search-AzGraph -Query $Query -UseTenantScope
11
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	: 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	: mg-sandboxes-corp-policytesting
id	: /providers/Microsoft.Management/managementGroups/mg-sandboxes-onlin
e	: mg-sandboxes-online
name	: mg-sandboxes-online
properties_displayName	: Sandboxes_Online
mgParent	: @{displayName=Tenant Root Group; name=f0fa27a0-8e7c-4f63-9a77-ec947
86b7c9e}	: 2
MGHierarchy	: f0fa27a0-8e7c-4f63-9a77-ec94786b7c9e
mgParent_name	: /providers/Microsoft.Management/managementGroups/mg-sandboxes-onlin
ResourceId	: e



Search - AzGraph (01:48)

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
[untested.ps1] Demo - Windows.ps1 BuildManifest PublishToGallery.ps1
425
426 # Get Azure Policy Assignments
427 #
428 Write-Output "Getting Policy Assignments from Azure Resource Graph using TenantScope"
429 $AzPolicyAssignments = @()
430
431 $pageSize = 1000
432 $iteration = 0
433 $searchParams = @{
434     Query = "policyresources `n
435             | where type == 'microsoft.authorization/policyassignments' "
436     First = $pageSize
437 }
438
439 $results = do {
440     $iteration += 1
441     $pageResults = Search-AzGraph @searchParams -UseTenantScope
442     $searchParams.Skip += $pageResults.Count
443     $AzPolicyAssignments += $pageResults
444 } while ($pageResults.Count -eq $pageSize)
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
```

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)

The screenshot shows a Windows PowerShell window titled "Administration Windows PowerShell ISE". The window contains a script with the following content:

```
25
26
27 ##### ShowQueryOnly in interactive mode
28 # ShowQueryOnly in interactive mode
29 #####
30
31 Query-AzResourceGraph -ShowQueryOnly
32
33 # we might need to login
34 # we can now see available pre-defined queries
35 # when we chose a query, it will ONLY show the query (not run)
36
37
```

Below the script, the PowerShell prompt "PS C:\>" is visible. The status bar at the bottom right indicates "Ch 20 Col 1" and "8085".



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

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1 Demo - Windows.ps1 BuildManifestsAndPSCoreGallery.ps1
562 #####
563 ##### Inspiration | Examples of use cases of data from Azure Resource Graph
564 # Data can be used as part of Reports, Alerts, Dashboards, workbooks
565 #####
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)

Availability Monitoring (ResourceH...)

Private dashboard

Auto refresh: Every 5 minutes UTC Time: Past 24 hours

Last updated: a few seconds ago

VMName	↑ availabilityState	↑ previousAvailabilityState	↑ occurredTime
sqlmonitorcollector	Unavailable	Unavailable	2023-06-17T12:45:13.8530000Z
DC1	Available	Available	2023-06-17T06:06:13.2880000Z
Mgmt1	Available	Available	2023-06-17T04:45:24.8830000Z
sqldemo1	Available	Available	2023-06-17T03:38:32.7920000Z
DC3	Available	Unavailable	2023-06-17T10:21:31.5860000Z

Virtual machines

DC3

Virtual machine | Directory: 2LINKIT

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks

Operations

- Bastion

Essentials

Resource group (move) : azurerg1-production-westeurope
 Status : Running
 Location : West Europe
 Subscription (move) : 2LINKIT CLOUD (MS SPONSORSHIP)
 Subscription ID : fce4f282-fcc6-43fb-94d8-bf1701b8...
 Operating system : Windows (Windows Server 2019 Da...
 Size : Standard B2ms (2 vcpus, 8 GiB mem...
 Public IP address :
 Virtual network/subnet : VNet1/Frontend
 DNS name :
 Health state :
 Tags (edit) : Click here to add tags

Properties **Monitoring** **Capabilities (8)** **Recommendations (1)** **Tutorials**

Virtual machine

- Computer name: DC3
- Operating system: Windows (Windows Server 2019 Datacenter)
- Image publisher: MicrosoftWindowsServer

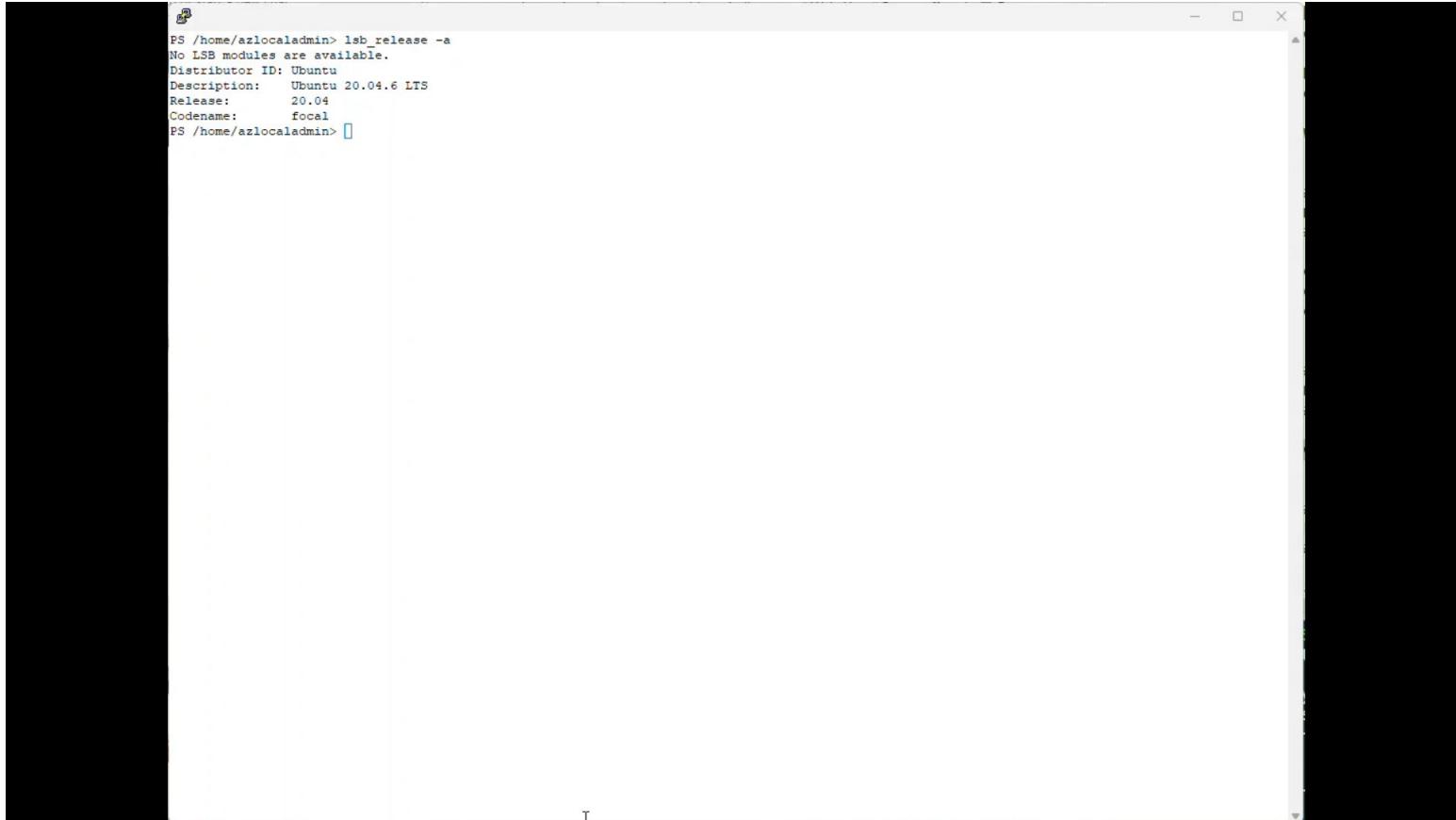


Azure Resource Graph Query

```
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

(01:11)



```
PS /home/azlocaladmin> lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.6 LTS
Release:        20.04
Codename:       focal
PS /home/azlocaladmin>
```

Azure LogAnalytics integration against Azure Resource Graph

```
1 InsightsMetrics           ← LogAnalytics table
2 | where Name == "UtilizationPercentage"
3 | summarize TimeGenerated = arg_max(TimeGenerated,*) by Computer
4 | lookup (
5 |     arg("").Resources   ← Lookup in ARG table
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
```

...

Results	Chart
Computer	ProcessorUtilization
> Mgmt1	36
> DC3	12
> DC1	11



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

log-platform-management-srvnetworkcloud-p | Logs

Log Analytics workspace | Directory: 2linkIT

New Query 1* New Query 2* New Query 3*

Azure Resource Graph table (scoping)

log-platform-man... Select scope Run Timerange: Set in query Save Share New alert rule Export Pin to Format query

```

1 arg("").Resources
2 | where type == "microsoft.compute/virtualmachines" and properties.hardwareProfile.vmSize startswith "Standard_B"
3 | join (InsightsMetrics
4 | | where TimeGenerated > ago(7d)
5 | | where Name == "UtilizationPercentage"
6 | | summarize AverageProcessorUtilizationPercentage = avg(Val) by Computer
7 | | on $left.name == $right.Computer
8 | project VMname=name, Location=location, SubscriptionId=subscriptionId, round(AverageProcessorUtilizationPercentage,0)

```

Join with LogAnalytics table

Results

VMname	Location	SubscriptionId	AverageProcessorUtilizationPercentage
DC3	westeurope	fce4f282-fcc6-43fb-94d8-bf170...	5
DC1	westeurope	fce4f282-fcc6-43fb-94d8-bf170...	10

Schema and Filter

▶ Run

Time range : Last 24 hours



Save



Share



New alert rule



Export



Pin to



Format query

```
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, ProcessorUtilizationPercentage=round(Val,0), tags
11 | .sort .by ProcessorUtilizationPercentage .desc
```

Azure dashboard

Grafana dashboard

Send to workbook

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



Time range : Last 24 hours



+ 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



Columns

Computer	ProcessorUtilization
> Mgmt1	36
> DC3	12
> DC1	11

4s 365ms

Display time (UTC+02:00)

Query details

1 - 3 of 3



Daily Backup Status Mail

(01:37)

```
#-----  
29     write-Output ""  
30     Write-Output "Collecting jobs status from RSV vaults .... Please Wait !!"  
31     $pageSize = 1000  
32     $searchParams = @{  
33         Query = "recoveryservicesresources`  
34             | where type == "microsoft.recoveryservices/vaults/backupjobs`"  
35             | where properties.startTime >= ago(1d)  
36             | where properties.operation != "ConfigureBackup`"  
37         First = $pageSize  
38     }  
39  
40     $Results = Search-AZGraph @searchParams -ManagementGroup $TenantId  
41     $RSVVaultJobStatus = $Results  
42  
43     Write-Output "Building statistics for Azure Recovery Vaults .... Please wait !!"  
44     If ($RSVVaultJobStatus)  
45     {  
46         $RSVCompletedJobs += $RSVVaultJobStatus | Where-Object({$_.properties.status -eq 'Completed'})
```

DataSourceName : 2linkitscriptsbackup
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>

Get Started with AzResourceGroupPS (Github)



P r e s e n t a t i o n
w i t h d e m o ' 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>