functional

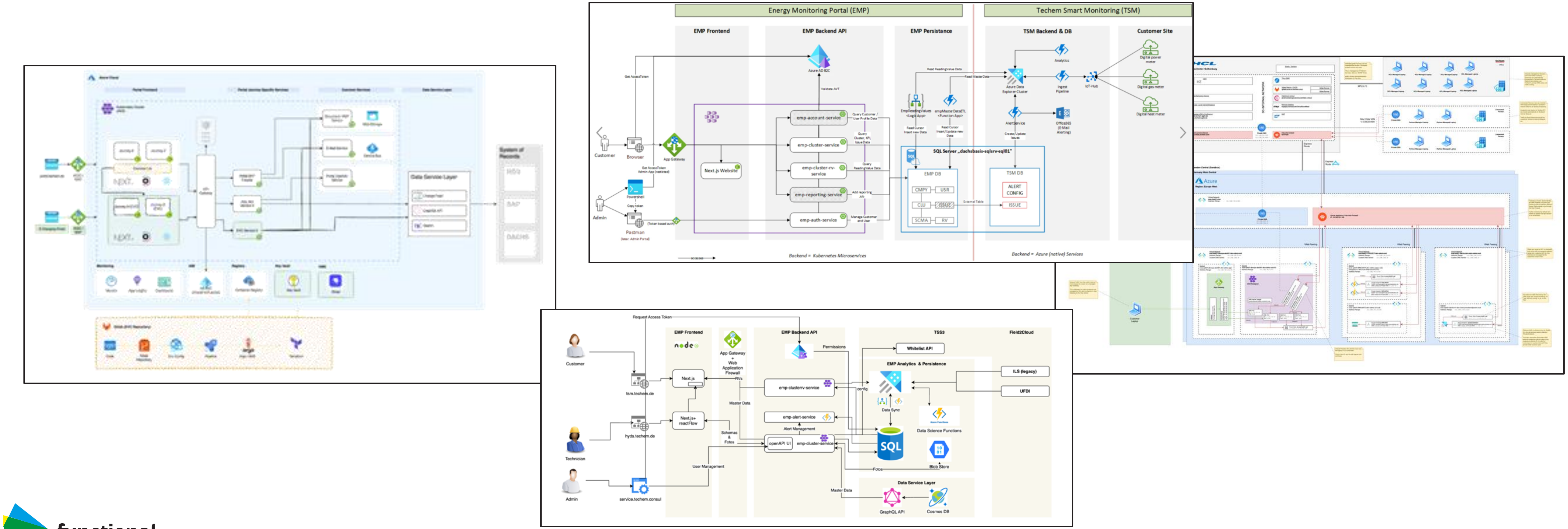
Herdings Cats with Azure Resource Graph

www.functional.team

AZURE RESOURCE GRAPH

Complexity Kills

- Many Enterprise Cloud Accounts are a hot mess.
- Hundreds of Subscriptions, Thousands of Resource Groups and deployed artifacts



AZURE RESOURCE GRAPH

Complexity Kills

Lack of transparency ~~can be~~ is a huge issue.

Maintenance impaired

Hand Overs delayed

Security jeopardized

Compliance questioned

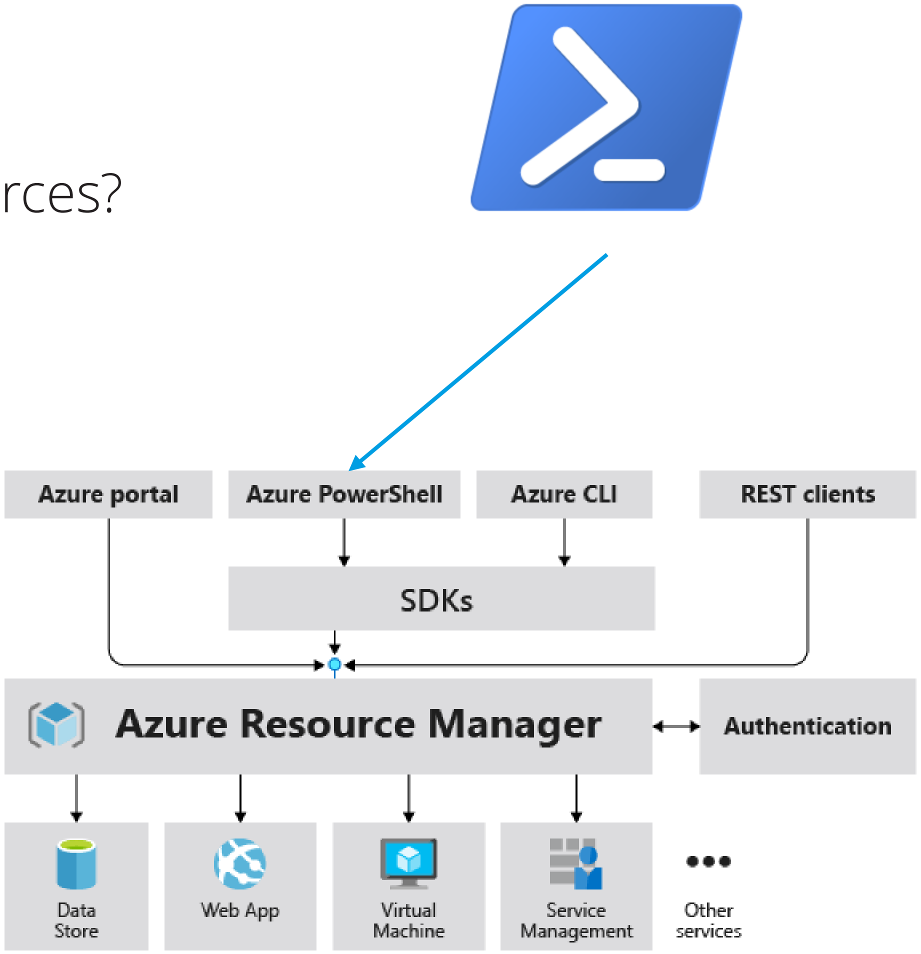
Custom Resource Crawling

- What’s do we have is deployed?
- What are the configs / properties across all my resources?
- Does my documentation correctly represent reality?

- We have Resource Manager APIs
- We can build scripts.

- Let’s use PowerShell, bash or Python
- Dump results into files or a database…

- Throttling can be a PITA.

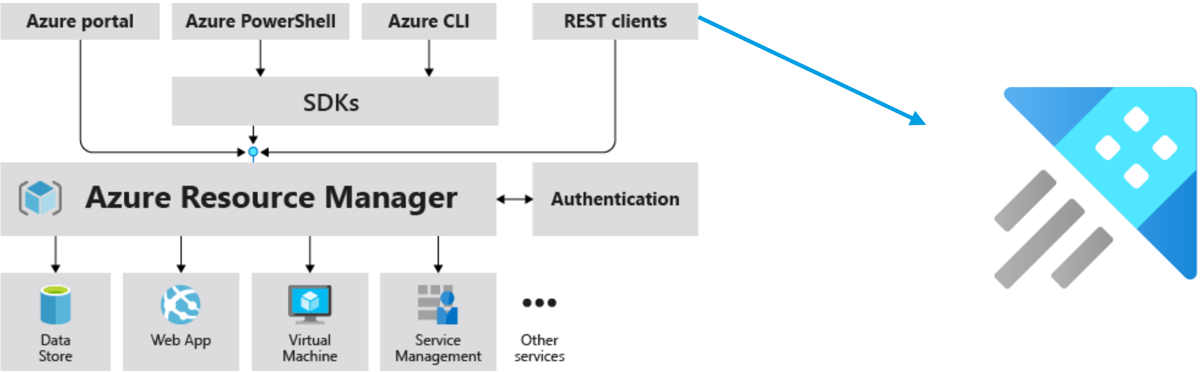


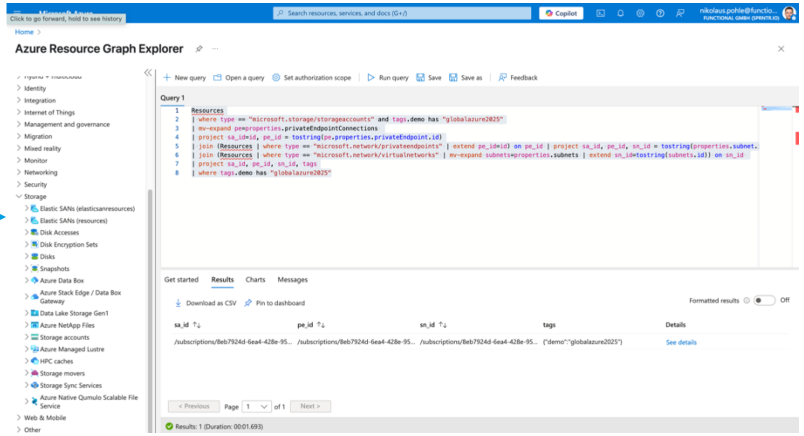
AZURE RESOURCE GRAPH

Resource Crawling As A Service

Turn’s out: Microsoft already did this for us.

-> Resource Graph continuously crawls Resource Provider APIs and stores the output in a KQL DB.





```
Resources
| where type == "microsoft.storage/storageaccounts" and tags.demo has "globalazure2025"
| mv-expand pe=properties.privateEndpointConnections
| project sa_id=id, pe_id = tostring(pe.properties.privateEndpoint.id)
| join (Resources | where type == "microsoft.network/privateendpoints" | extend pe_id=id) on pe_id | project sa_id, pe_id, sn_id = tostring(properties.subnet.
| join (Resources | where type == "microsoft.network/virtualnetworks" | mv-expand subnets=properties.subnets | extend sn_id=tostring(subnets.id)) on sn_id
| project sa_id, pe_id, sn_id, tags
| where tags.demo has "globalazure2025"
```

sa_id ↑↓	pe_id ↑↓	sn_id ↑↓	tags	Details
/subscriptions/8eb7924d-6ea4-428e-95...	/subscriptions/8eb7924d-6ea4-428e-95...	/subscriptions/8eb7924d-6ea4-428e-95...	{"demo":"globalazure2025"}	See details

Results: 1 (Duration: 00:01.693)

functional

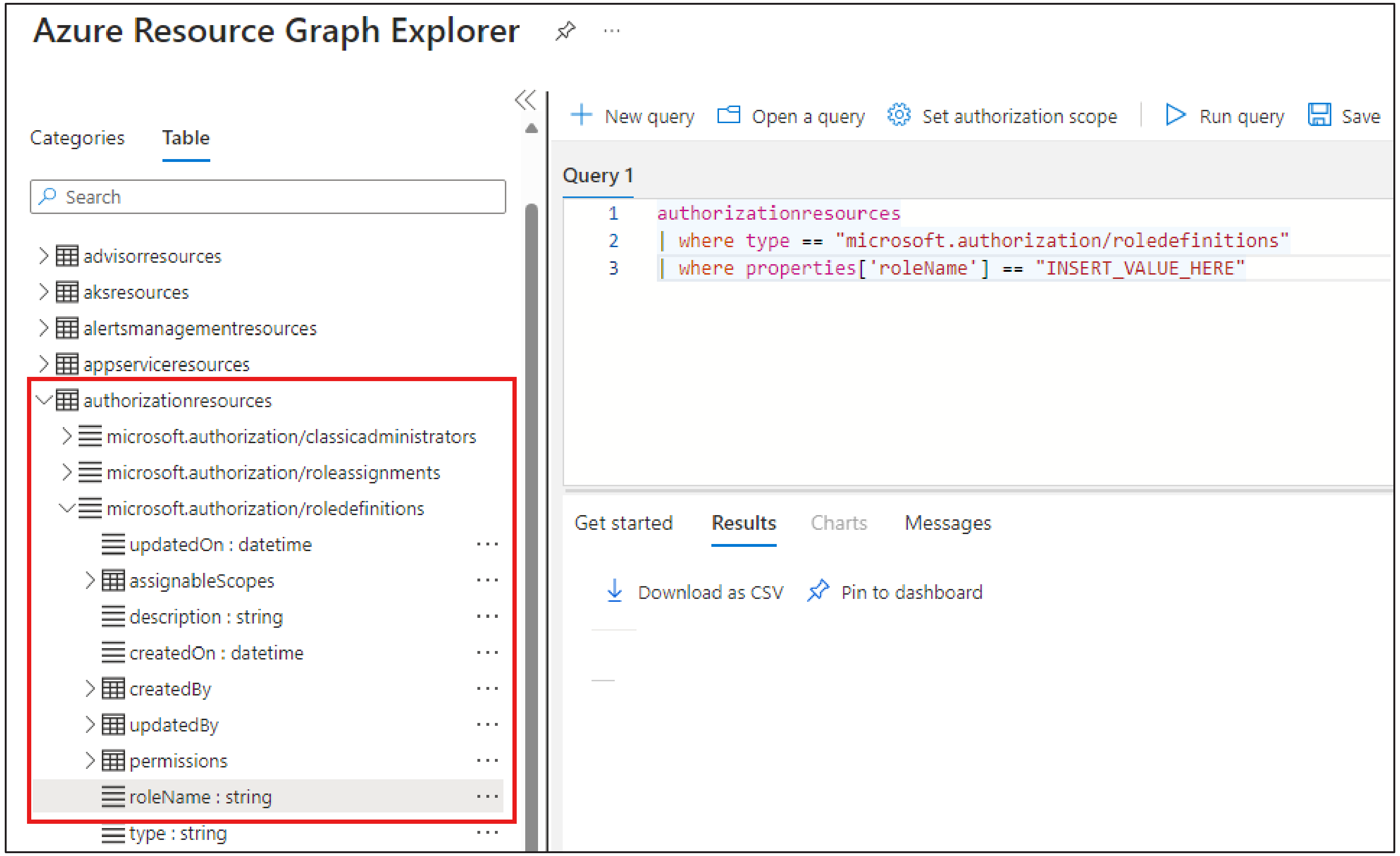
AZURE RESOURCE GRAPH

Extensive Coverage of Resource Types

advisorresources
aksresources
alertsmanagementresources
appserviceresources
authorizationresources
awsresources
azurebusinesscontinuityresources
azuredevopsplatformresources
batchresources
capabilityresources
chaosresources
communitygalleryresources
computeresources
deploymentresources
desktopvirtualizationresources
dnsresources
edgeorderresources
elasticsanresources
extendedlocationresources
extensibilityresourcechanges
featureresources
guestconfigurationresources
healthresourcechanges
healthresources
impactreportresources
insightresources
iotsecurityresources
kubernetesconfigurationresources
kustoresources
maintenanceresourcechanges
maintenanceresources
managedserviceresources
mirgateresources
networkresourcechanges
networkresources
orbitalresources
patchassessmentresources
patchinstallationresources
policyresources
quotaresourcechanges
recoveryservicesresources
resourcechanges
resourcecontainerchanges
resourcecontainers
resources
securityresources
servicefabricresources
servicehealthresources
sportresources
tagresources

AZURE RESOURCE GRAPH

Visual Schema Explorer



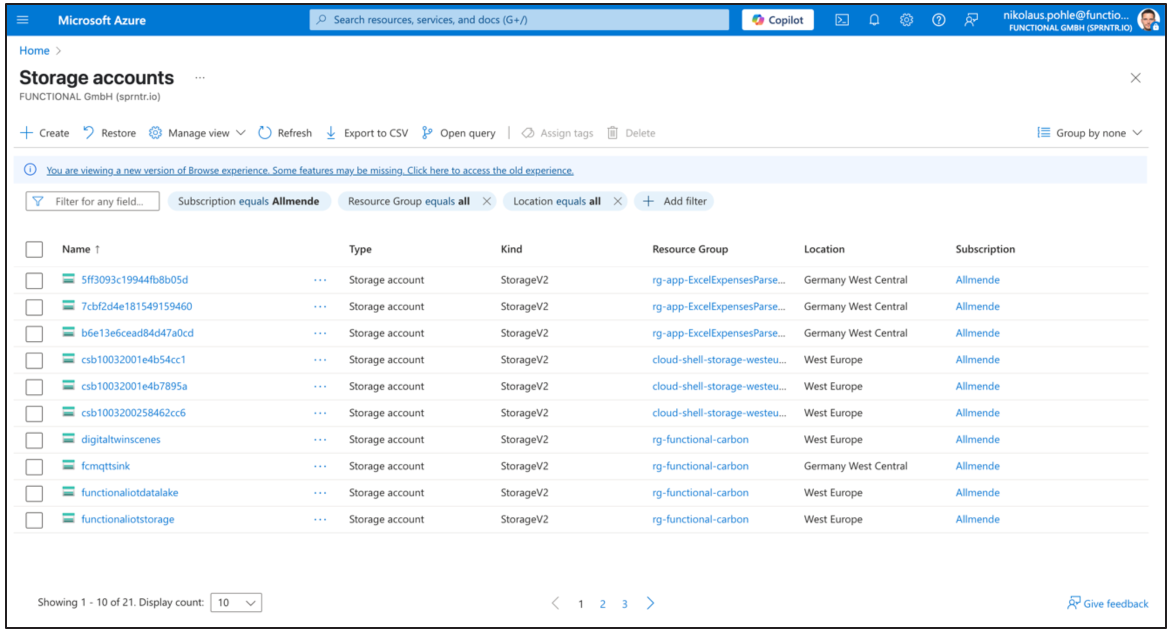
```
authorizationresources
| where type == "microsoft.authorization/roledefinitions"
| where properties['roleName'] == "INSERT_VALUE_HERE"
```

functional

AZURE RESOURCE GRAPH

Eat Your Own Dogfood

Azure Portal does use Resource Graph Queries extensively.



Storage accounts

FUNCTIONAL GmbH (sprntr.io)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

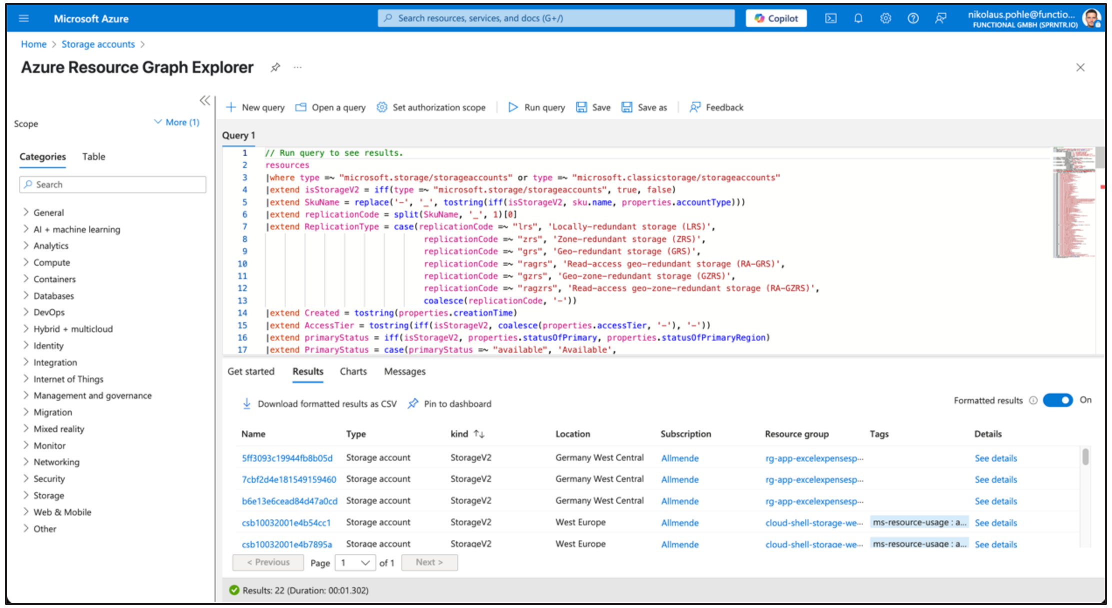
Subscription equals **Allmende** | Resource Group equals **all** | Location equals **all**

Name ↑	Type	Kind	Resource Group	Location	Subscription
5ff3093c19944fb8b05d	Storage account	StorageV2	rg-app-ExcelExpensesParse...	Germany West Central	Allmende
7cbf2d4e181549159460	Storage account	StorageV2	rg-app-ExcelExpensesParse...	Germany West Central	Allmende
b6e13e6cead84d47a0cd	Storage account	StorageV2	rg-app-ExcelExpensesParse...	Germany West Central	Allmende
csb10032001e4b54cc1	Storage account	StorageV2	cloud-shell-storage-westeu...	West Europe	Allmende
csb10032001e4b7895a	Storage account	StorageV2	cloud-shell-storage-westeu...	West Europe	Allmende
csb1003200258462cc6	Storage account	StorageV2	cloud-shell-storage-westeu...	West Europe	Allmende
digitaltwinscenes	Storage account	StorageV2	rg-functional-carbon	West Europe	Allmende
fcmqttsink	Storage account	StorageV2	rg-functional-carbon	Germany West Central	Allmende
functionaliotdatalake	Storage account	StorageV2	rg-functional-carbon	West Europe	Allmende
functionaliotstorage	Storage account	StorageV2	rg-functional-carbon	West Europe	Allmende

Showing 1 - 10 of 21. Display count: 10

< 1 2 3 >

Give feedback



Azure Resource Graph Explorer

```
// Run query to see results.
resources
|where type =~ "microsoft.storage/storageaccounts" or type =~ "microsoft.classicstorage/storageaccounts"
|extend isStorageV2 = iff(type =~ "microsoft.storage/storageaccounts", true, false)
|extend SkuName = replace('-', '_', tostring(iff(isStorageV2, sku.name, properties.accountType)))
|extend replicationCode = split(SkuName, '_', 1)[0]
|extend ReplicationType = case(replicationCode =~ "lrs", 'Locally-redundant storage (LRS)',
                               replicationCode =~ "zrs", 'Zone-redundant storage (ZRS)',
                               replicationCode =~ "grs", 'Geo-redundant storage (GRS)',
                               replicationCode =~ "ragrs", 'Read-access geo-redundant storage (RA-GRS)',
                               replicationCode =~ "gzrs", 'Geo-zone-redundant storage (GZRS)',
                               replicationCode =~ "ragzrs", 'Read-access geo-zone-redundant storage (RA-GZRS)',
                               coalesce(replicationCode, '-'))
|extend Created = tostring(properties.creationTime)
|extend AccessTier = tostring(iff(isStorageV2, coalesce(properties.accessTier, '-'), '-'))
|extend primaryStatus = iff(isStorageV2, properties.statusOfPrimary, properties.statusOfPrimaryRegion)
|extend PrimaryStatus = case(primaryStatus =~ "available", 'Available',
```

Name	Type	kind ↑↓	Location	Subscription	Resource group	Tags	Details
5ff3093c19944fb8b05d	Storage account	StorageV2	Germany West Central	Allmende	rg-app-excelexpensesp...		See details
7cbf2d4e181549159460	Storage account	StorageV2	Germany West Central	Allmende	rg-app-excelexpensesp...		See details
b6e13e6cead84d47a0cd	Storage account	StorageV2	Germany West Central	Allmende	rg-app-excelexpensesp...		See details
csb10032001e4b54cc1	Storage account	StorageV2	West Europe	Allmende	cloud-shell-storage-we...	ms-resource-usage : a...	See details
csb10032001e4b7895a	Storage account	StorageV2	West Europe	Allmende	cloud-shell-storage-we...	ms-resource-usage : a...	See details

< Previous Page 1 of 1 Next >

Results: 22 (Duration: 00:01.302)

functional

AZURE RESOURCE GRAPH

Demo Time: Query The Graph

- Find all Storage Accounts with a specific tag
- Filter down on Storage Accounts that have a private endpoint configured
- Find the associated Virtual Network / Subnet
- Check if the subnet is tagged accordingly

```
Resources
| where type == "microsoft.storage/storageaccounts" and tags.demo has "globalazure2025"
| mv-expand pe=properties.privateEndpointConnections
| project sa_id=id, pe_id = tostring(pe.properties.privateEndpoint.id)
| join (Resources | where type == "microsoft.network/privateendpoints" | extend pe_id=id) on pe_id | project sa_id, pe_id, sn_id = tostring(properties.subnet.id)
| join (Resources | where type == "microsoft.network/virtualnetworks" | mv-expand subnets=properties.subnets | extend sn_id=tostring(subnets.id)) on sn_id
| project sa_id, pe_id, sn_id, tags
| where tags.demo has "globalazure2025"
```

AZURE RESOURCE GRAPH

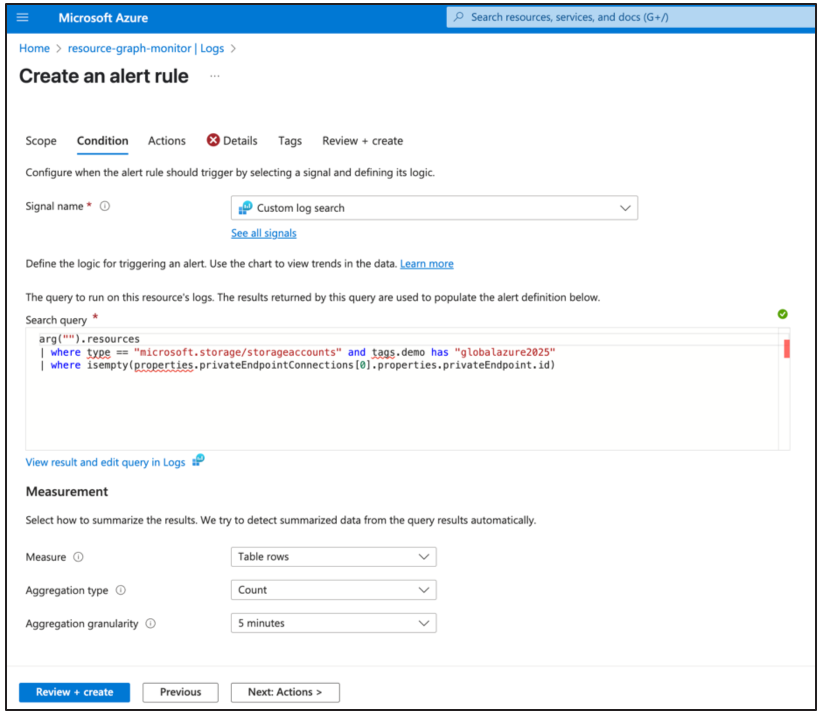
Graph-based Alerts

- Alert me if a tagged Storage Account is lacking a Private Endpoint / Vnet integration.

```
arg("").resources
| where type == "microsoft.storage/storageaccounts" and tags.demo has "globalazure2025"
| where isempty(properties.privateEndpointConnections[0].properties.privateEndpoint.id)
```

Attention:

Complex Queries / JOINS might not work here



Create an alert rule

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name *: Custom log search

Define the logic for triggering an alert. Use the chart to view trends in the data.

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
arg("").resources
| where type == "microsoft.storage/storageaccounts" and tags.demo has "globalazure2025"
| where isempty(properties.privateEndpointConnections[0].properties.privateEndpoint.id)
```

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure: Table rows

Aggregation type: Count

Aggregation granularity: 5 minutes

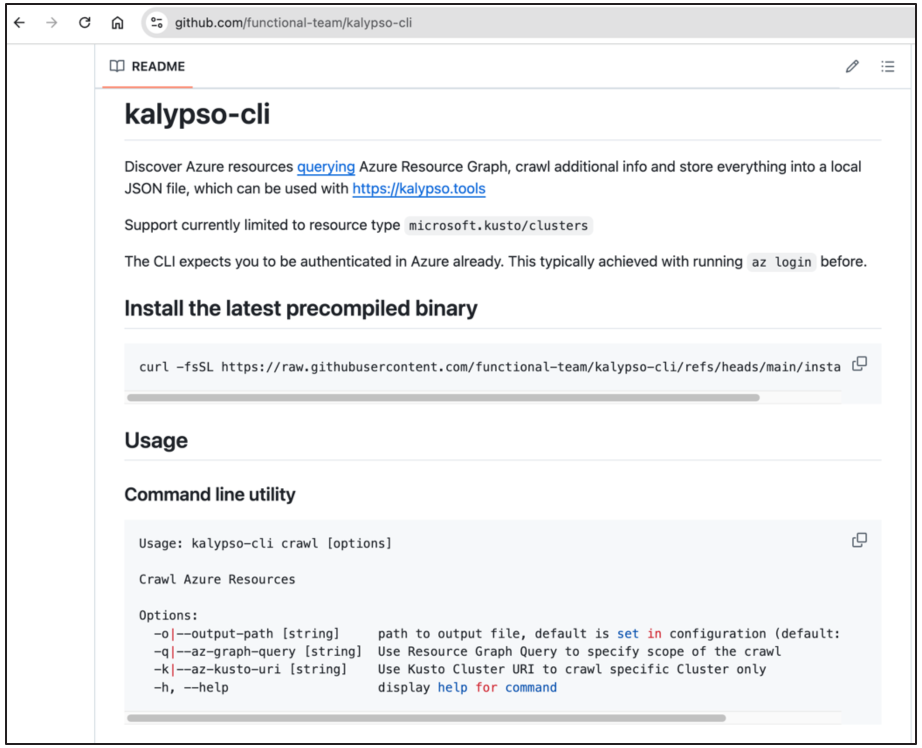
AZURE RESOURCE GRAPH

KALYPSO: Resource Crawling 2.0

- Leverage Azure Resource Graph Queries in custom tools to maximize the potential.

- run custom ARG queries
- Fetch additional context
- Dump everything into a local json file

- Diff versions of the file to have a change log
- Find dependencies between resources
- Visualize dependencies and properties



kalypso-cli

Discover Azure resources querying Azure Resource Graph, crawl additional info and store everything into a local JSON file, which can be used with https://kalypso.tools

Support currently limited to resource type `microsoft.kusto/clusters`

The CLI expects you to be authenticated in Azure already. This typically achieved with running `az login` before.

Install the latest precompiled binary

```
curl -fsSL https://raw.githubusercontent.com/functional-team/kalypso-cli/refs/heads/main/insta
```

Usage

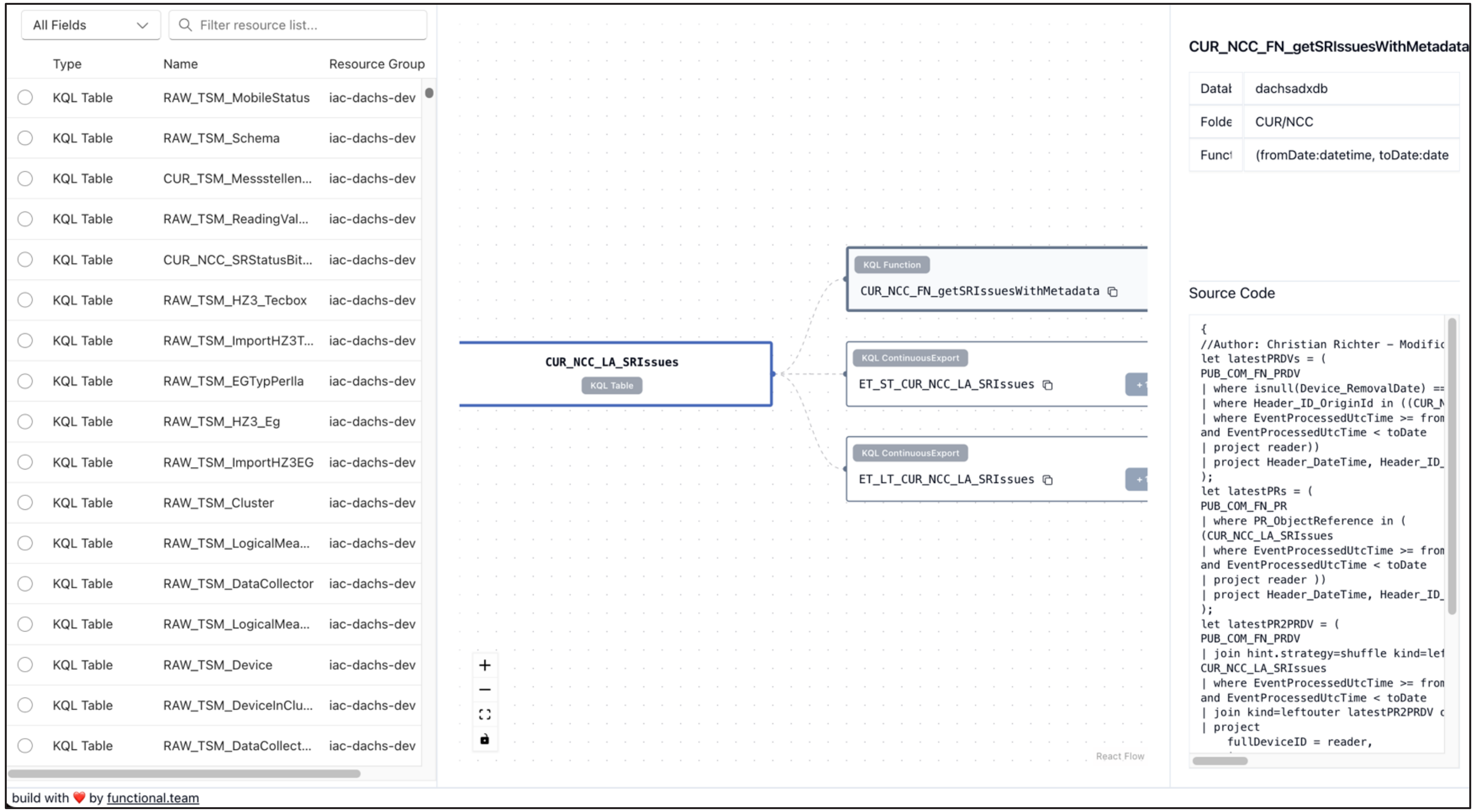
Command line utility

```
Usage: kalypso-cli crawl [options]

Crawl Azure Resources

Options:
  -o|--output-path [string]     path to output file, default is set in configuration (default:
  -q|--az-graph-query [string]  Use Resource Graph Query to specify scope of the crawl
  -k|--az-kusto-uri [string]    Use Kusto Cluster URI to crawl specific Cluster only
  -h, --help                    display help for command
```

functional

AZURE RESOURCE GRAPH

Explore Resources



	Type	Name	Resource Group
○	KQL Table	RAW_TSM_MobileStatus	iac-dachs-dev
○	KQL Table	RAW_TSM_Schema	iac-dachs-dev
○	KQL Table	CUR_TSM_Messstellen...	iac-dachs-dev
○	KQL Table	RAW_TSM_ReadingVal...	iac-dachs-dev
○	KQL Table	CUR_NCC_SRStatusBit...	iac-dachs-dev
○	KQL Table	RAW_TSM_HZ3_Tecbox	iac-dachs-dev
○	KQL Table	RAW_TSM_ImportHZ3T...	iac-dachs-dev
○	KQL Table	RAW_TSM_EGTypPerlla	iac-dachs-dev
○	KQL Table	RAW_TSM_HZ3_Eg	iac-dachs-dev
○	KQL Table	RAW_TSM_ImportHZ3EG	iac-dachs-dev
○	KQL Table	RAW_TSM_Cluster	iac-dachs-dev
○	KQL Table	RAW_TSM_LogicalMea...	iac-dachs-dev
○	KQL Table	RAW_TSM_DataCollector	iac-dachs-dev
○	KQL Table	RAW_TSM_LogicalMea...	iac-dachs-dev
○	KQL Table	RAW_TSM_Device	iac-dachs-dev
○	KQL Table	RAW_TSM_DeviceInClu...	iac-dachs-dev
○	KQL Table	RAW_TSM_DataCollect...	iac-dachs-dev

CUR_NCC_LA_SRIssues

CUR_NCC_FN_getSRIssuesWithMetadata

ET_ST_CUR_NCC_LA_SRIssues

ET_LT_CUR_NCC_LA_SRIssues

CUR_NCC_FN_getSRIssuesWithMetadata

Datal	dachsadxdb
Folde	CUR/NCC
Funct	(fromDate:datetime, toDate:date

Source Code

```
{
//Author: Christian Richter - Modific
let latestPRDVs = (
PUB_COM_FN_PRDV
| where isnull(Device_RemovalDate) ==
| where Header_ID_OriginId in ((CUR_N
| where EventProcessedUtcTime >= fron
and EventProcessedUtcTime < toDate
| project reader))
| project Header_DateTime, Header_ID_
);
let latestPRs = (
PUB_COM_FN_PR
| where PR_ObjectReference in (
(CUR_NCC_LA_SRIssues
| where EventProcessedUtcTime >= fron
and EventProcessedUtcTime < toDate
| project reader ))
| project Header_DateTime, Header_ID_
);
let latestPR2PRDV = (
PUB_COM_FN_PRDV
| join hint.strategy=shuffle kind=lef
CUR_NCC_LA_SRIssues
| where EventProcessedUtcTime >= fron
and EventProcessedUtcTime < toDate
| join kind=leftouter latestPR2PRDV c
| project
    fullDeviceID = reader,
```

functional

functional

Nikolaus Pohle
Managing Director

Drostestraße 16 . 30161 Hannover

www.functional.team
hello@functional.team

www.functional.team