KQL Query Library - Complete Azure Resource Graph Reference

Cost Analysis Queries

Find Untagged Resources by Subscription

```
Resources
| where tags !has 'Environment' or tags !has 'CostCenter' or tags !has 'C
| summarize Count=count() by subscriptionId, type
| order by Count desc
```

Calculate Monthly Costs by Tag

```
Resources
| where type =~ 'microsoft.compute/virtualmachines'
| extend Environment = tostring(tags['Environment']),
         CostCenter = tostring(tags['CostCenter'])
| join kind=inner (
    consumptionusage
    | where ResourceType == 'microsoft.compute/virtualmachines'
    | summarize MonthlyCost = sum(PreTaxCost) by ResourceId
) on $left.id == $right.ResourceId
| summarize TotalCost = sum(MonthlyCost) by Environment, CostCenter
| order by TotalCost desc
```

Orphaned Disks (Cost Recovery)

```
Resources
| where type =~ 'microsoft.compute/disks'
| where properties.diskState == 'Unattached'
| extend diskSizeGB = properties.diskSizeGB,
         sku = properties.sku.name
| extend monthlyCost = case(
```

```
    sku == 'Premium_LRS', diskSizeGB * 0.16,
    sku == 'StandardSSD_LRS', diskSizeGB * 0.08,
    diskSizeGB * 0.05
  )
| project id, name, resourceGroup, subscriptionId,
        diskSizeGB, sku, monthlyCost
| order by monthlyCost desc
```

Old Snapshots (>90 days)

```
Resources
| where type =~ 'microsoft.compute/snapshots'
| extend createdTime = properties.timeCreated
| extend ageInDays = datetime_diff('day', now(), todatetime(createdTime))
| where ageInDays > 90
| extend diskSizeGB = properties.diskSizeBytes / 1073741824
| extend monthlyCost = diskSizeGB * 0.05
| project id, name, resourceGroup, ageInDays, monthlyCost
| order by ageInDays desc
```

Security & Compliance Queries

VMs Without Azure Monitor Agent

```
Resources
| where type =~ 'microsoft.compute/virtualmachines'
| where properties.provisioningState == 'Succeeded'
| extend vmId = tolower(id)
| join kind=leftouter (
    Resources
    | where type =~ 'microsoft.compute/virtualmachines/extensions'
    | where name == 'AzureMonitorLinuxAgent' or name == 'AzureMonitorWind
    | extend vmId = tolower(substring(id, 0, indexof(id, '/extensions')))
    | project vmId, extensionName = name
) on vmId
| where isnull(extensionName)
| project name, resourceGroup, subscriptionId, location
```

Public IP Addresses (Security Audit)

```
Resources
| where type =~ 'microsoft.network/publicipaddresses'
| extend ipAddress = properties.ipAddress
| where isnotempty(ipAddress)
| extend attachedTo = properties.ipConfiguration.id
| project name, ipAddress, attachedTo, resourceGroup, subscriptionId
```

NSG Rules Allowing Internet Access

```
Resources
| where type =~ 'microsoft.network/networksecuritygroups'
| mvexpand rules = properties.securityRules
| extend ruleName = rules.name,
         access = rules.properties.access,
         direction = rules.properties.direction,
         sourceAddress = rules.properties.sourceAddressPrefix
| where access == 'Allow'
  and direction == 'Inbound'
  and (sourceAddress == '*' or sourceAddress == 'Internet')
| project nsgName = name, ruleName, sourceAddress,
         destinationPort = rules.properties.destinationPortRange,
         resourceGroup
```

Performance & Inventory Queries

VM Inventory with SKU Details

```
Resources
| where type =~ 'microsoft.compute/virtualmachines'
| extend vmSize = properties.hardwareProfile.vmSize,
         osType = properties.storageProfile.osDisk.osType,
         imagePublisher = properties.storageProfile.imageReference.publis
         imageOffer = properties.storageProfile.imageReference.offer
| project name, vmSize, osType, imagePublisher, imageOffer,
         resourceGroup, subscriptionId, location, tags
```

Disk Performance Tiers

```
Resources
| where type =~ 'microsoft.compute/disks'
| extend diskSizeGB = properties.diskSizeGB,
         tier = properties.tier,
         sku = properties.sku.name,
         iops = properties.diskIOPSReadWrite,
         throughput = properties.diskMBpsReadWrite
| project name, diskSizeGB, tier, sku, iops, throughput,
         resourceGroup, subscriptionId
| order by iops desc
```

Storage Accounts by Type

```
Resources
| where type =~ 'microsoft.storage/storageaccounts'
| extend sku = properties.sku.name,
        kind = properties.kind,
        encryption = properties.encryption.services.blob.enabled
| project name, sku, kind, encryption, resourceGroup, subscriptionId
```

Network Analysis Queries

Virtual Networks with Subnets

```
Resources
| where type =~ 'microsoft.network/virtualnetworks'
| mvexpand subnets = properties.subnets
| extend subnetName = subnets.name,
        addressPrefix = subnets.properties.addressPrefix,
        nsgId = subnets.properties.networkSecurityGroup.id
| project vnetName = name, subnetName, addressPrefix, nsgId,
         resourceGroup, subscriptionId
```

Unattached Network Interfaces

```
Resources
| where type =~ 'microsoft.network/networkinterfaces'
| where isnull(properties.virtualMachine)
  and isnull(properties.privateEndpoint)
| extend privateIP = properties.ipConfigurations[0].properties.privateIPA
| project name, privateIP, resourceGroup, subscriptionId
```

ExpressRoute Circuits

```
Resources
| where type =~ 'microsoft.network/expressroutecircuits'
| extend provider = properties.serviceProviderProperties.serviceProviderN
         bandwidth = properties.serviceProviderProperties.bandwidthInMbps
         peeringLocation = properties.serviceProviderProperties.peeringLc
| project name, provider, bandwidth, peeringLocation, resourceGroup
```

Azure Arc Queries

Arc-Enabled Servers by OS

```
Resources
| where type =~ 'microsoft.hybridcompute/machines'
| extend osType = properties.osType,
         osVersion = properties.osVersion,
         status = properties.status
| summarize Count=count() by osType, status
| order by Count desc
```

Arc Server Last Heartbeat

```
Resources
| where type =~ 'microsoft.hybridcompute/machines'
| extend lastHeartbeat = todatetime(properties.lastStatusChange),
         status = properties.status
| extend daysSinceHeartbeat = datetime_diff('day', now(), lastHeartbeat)
| where daysSinceHeartbeat > 1
```

```
| project name, lastHeartbeat, daysSinceHeartbeat, status, resourceGroup
| order by daysSinceHeartbeat desc
```

Tag Governance Queries

Resources Missing Required Tags

```
Resources
| extend environment = tostring(tags['Environment']),
        costCenter = tostring(tags['CostCenter']),
        owner = tostring(tags['Owner']),
        application = tostring(tags['Application'])
| where isnull(environment) or isempty(environment)
    or isnull(costCenter) or isempty(costCenter)
    or isnull(owner) or isempty(owner)
    or isnull(application) or isempty(application)
| summarize Count=count() by type, resourceGroup
| order by Count desc
```

Tag Value Standardization Issues

```
Resources
| extend environment = tostring(tags['Environment'])
| where isnotempty(environment)
| summarize Count=count() by environment
| order by Count desc
```

Usage Instructions

Running Queries

1. **Azure Portal:**

   - Go to "Resource Graph Explorer"
   - Paste query
   - Click "Run query"

2. **Azure CLI:**
```bash
ash az graph query -q "YOUR_QUERY_HERE"
```

3. **PowerShell:**
```powershell
powershell Search-AzGraph -Query "YOUR_QUERY_HERE"
```

Best Practices

- Use project to limit returned columns
- Add | take 100 for testing large queries
- Use summarize for aggregations
- Join with consumptionusage for cost data
- Cache results for reporting dashboards

Common Filters

- By subscription: | where subscriptionId == '...'
- By resource group: | where resourceGroup == '...'
- By location: | where location == 'eastus'
- By tag: | where tags['Environment'] == 'Production'

Complete KQL Resources

For more detailed KQL guides and enterprise examples:

- https://azure-noob.com/blog/kql-cheat-sheet-complete
- https://azure-noob.com/blog/azure-vm-inventory-kql
- https://azure-noob.com/hub/kql

Azure Noob - December 2025

Production-tested queries from managing 44 Azure subscriptions