KQL|Cafe

Session 1 | Getting started

KQL Café | Mission

A Community to make the world a better place with KQL

Learn, share and practice the KQL language

Your | hosts

Your | hosts

Alex Verboon

Microsoft® MVP Most Valuable Professional

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Gianni Castaldi

https://twitter.com/castello_johnny

https://www.linkedin.com/in/giannicastaldi/

https://github.com/KustoKing

https://www.kustoking.com/

Today's | Guest

Today's | Guest

Rod Trent

Senior Cloud Security Advocate, Microsoft

My blog: https://aka.ms/RodsBlog
Must Learn KQL series: https://aka.ms/MustLearnKQL
GitHub: https://github.com/rod-trent
LinkedIn Profile: https://www.linkedin.com/in/rodtrent/
Twitter: https://twitter.com/rodtrent

Schedule | Registration

We plan to run the show on every 3rd Tuesday of the month

18:00 – 20:00 Central European Time

Sessions will be announced in Meetup

https://www.meetup.com/kql-cafe/

Show | Agenda

Where do we KQL?

Your Playground Options

KQL Basics | Top 8 Operators

KQL Tables | How to find new things

Working with IOCs

Features worth mentioning

Todays guest speaker: Rod Trent

What did you do with KQL this month?

KQL Challenge of the month

Where do we KQL?

Microsoft 365 Defender

Microsoft Sentinel

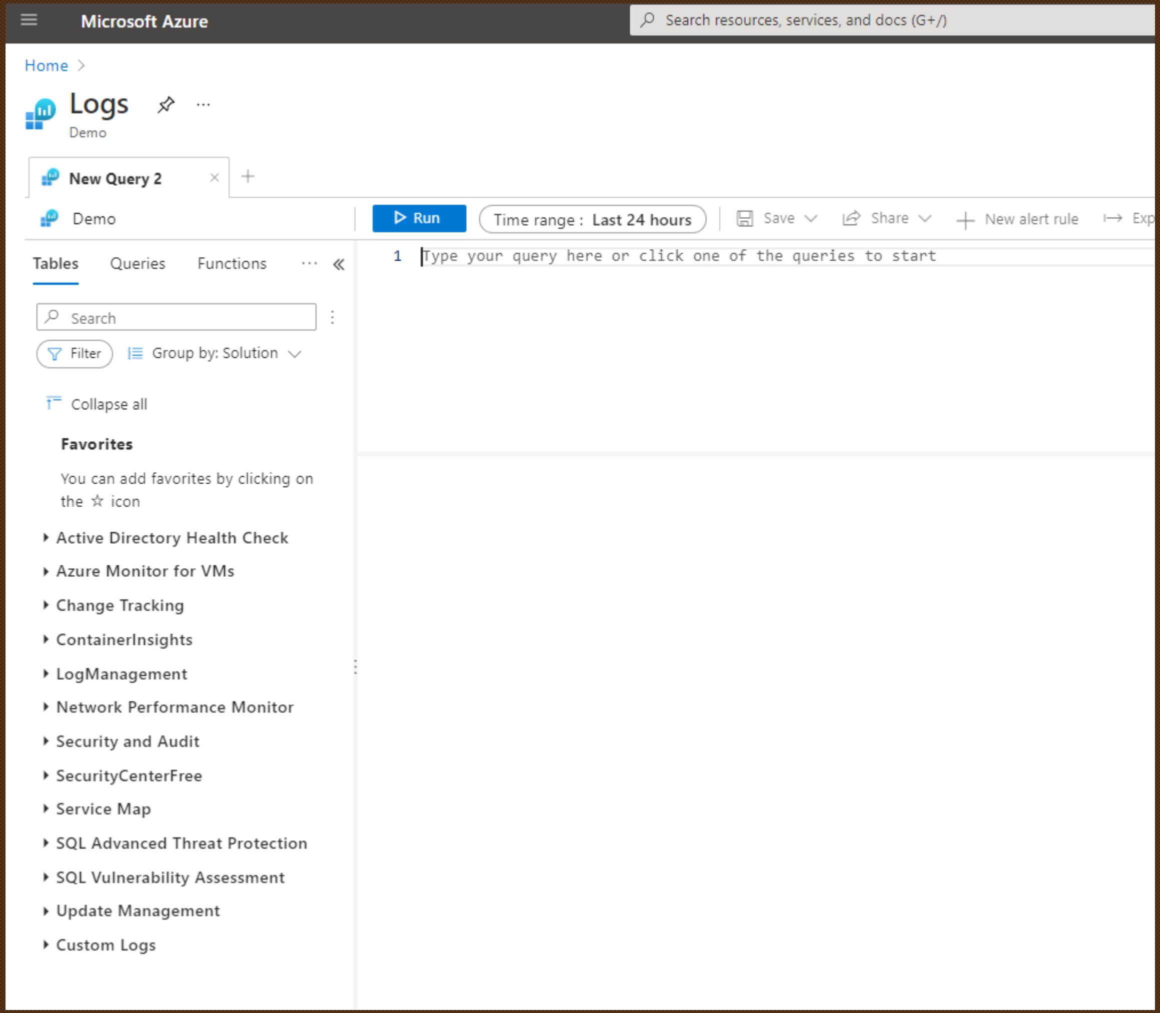
Log Analytics

Data Explorer

Microsoft Endpoint Configuration Manager (CMPivot)

Log Analytics Demo

https://aka.ms/lademo



Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Logs

Demo

New Query 2

Demo

Run

Time range : Last 24 hours

Save

Share

New alert rule

Exp

Tables Queries Functions

```
Type your query here or click one of the queries to start
```

Search

Filter

Group by: Solution

Collapse all

Favorites

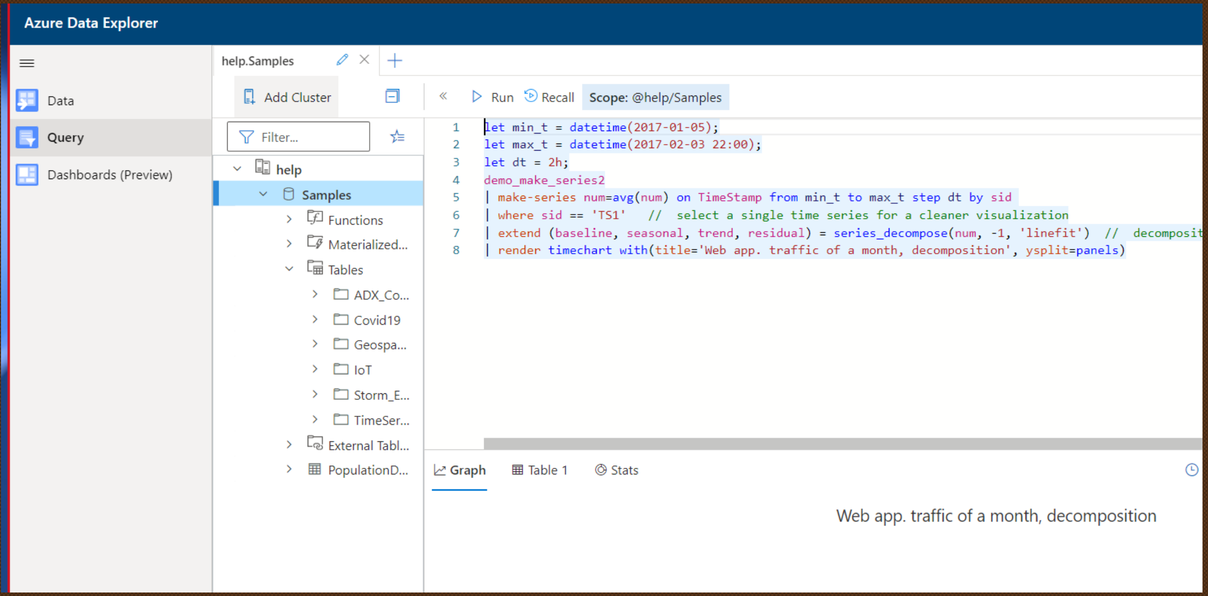
You can add favorites by clicking on the ☆ icon

- Active Directory Health Check
- Azure Monitor for VMs
- Change Tracking
- ContainerInsights
- LogManagement
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- Service Map
- SQL Advanced Threat Protection
- SQL Vulnerability Assessment
- Update Management
- Custom Logs

Your playground options

Azure Data Explorer

https://dataexplorer.azure.com/clusters/help/databases/Samples

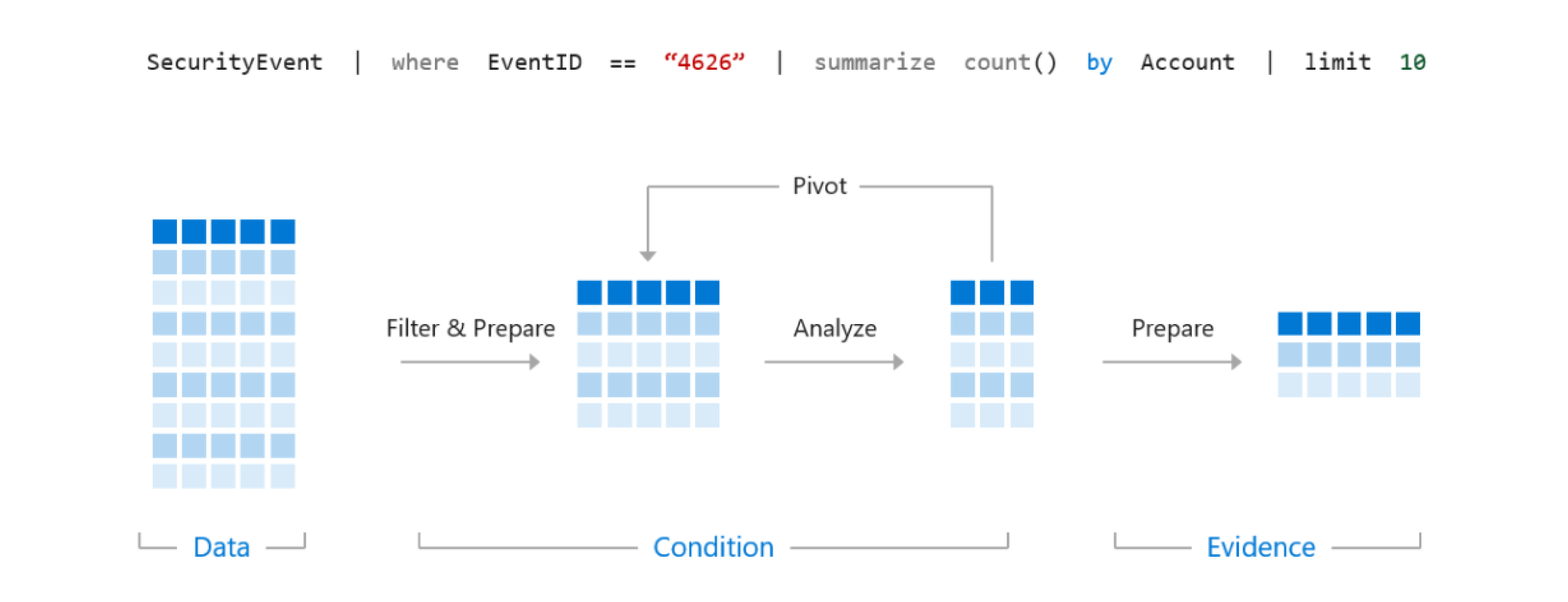


Scope: @help/Samples

```
let min_t = datetime(2017-01-05);
let max_t = datetime(2017-02-03 22:00);
let dt = 2h;
demo_make_series2
| make-series num=avg(num) on TimeStamp from min_t to max_t step dt by sid
| where sid == 'TS1'   //  select a single time series for a cleaner visualization
| extend (baseline, seasonal, trend, residual) = series_decompose(num, -1, 'linefit')  //  decomposit
| render timechart with(title='Web app. traffic of a month, decomposition', ysplit=panels)
```

Web app. traffic of a month, decomposition

KQL Basics | Top 8 operators



```
SecurityEvent | where EventID == “4626” | summarize count() by Account | limit 10
```

search

project

has <> contains

distinct

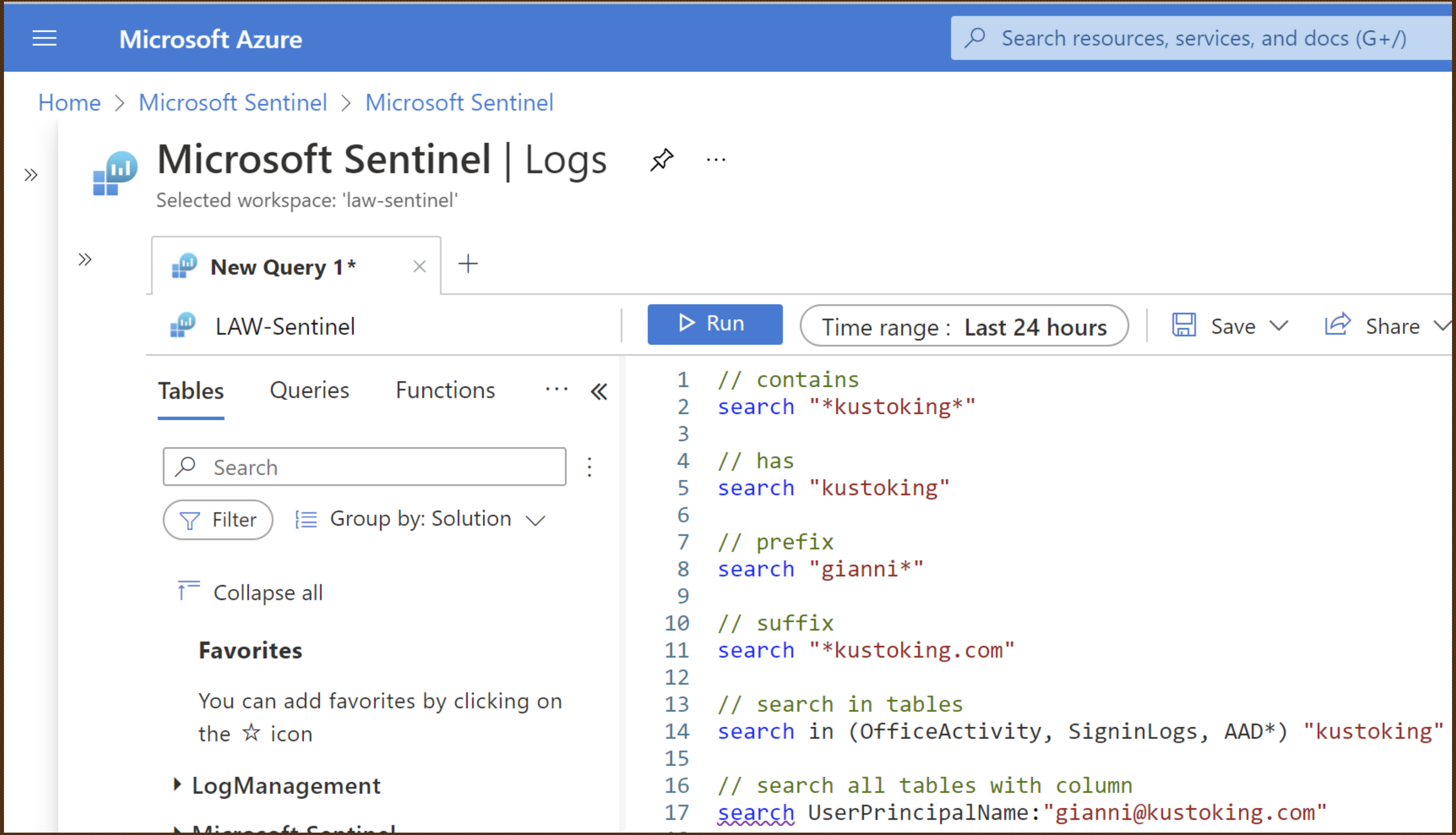
summarize

extend

take <> limit

join

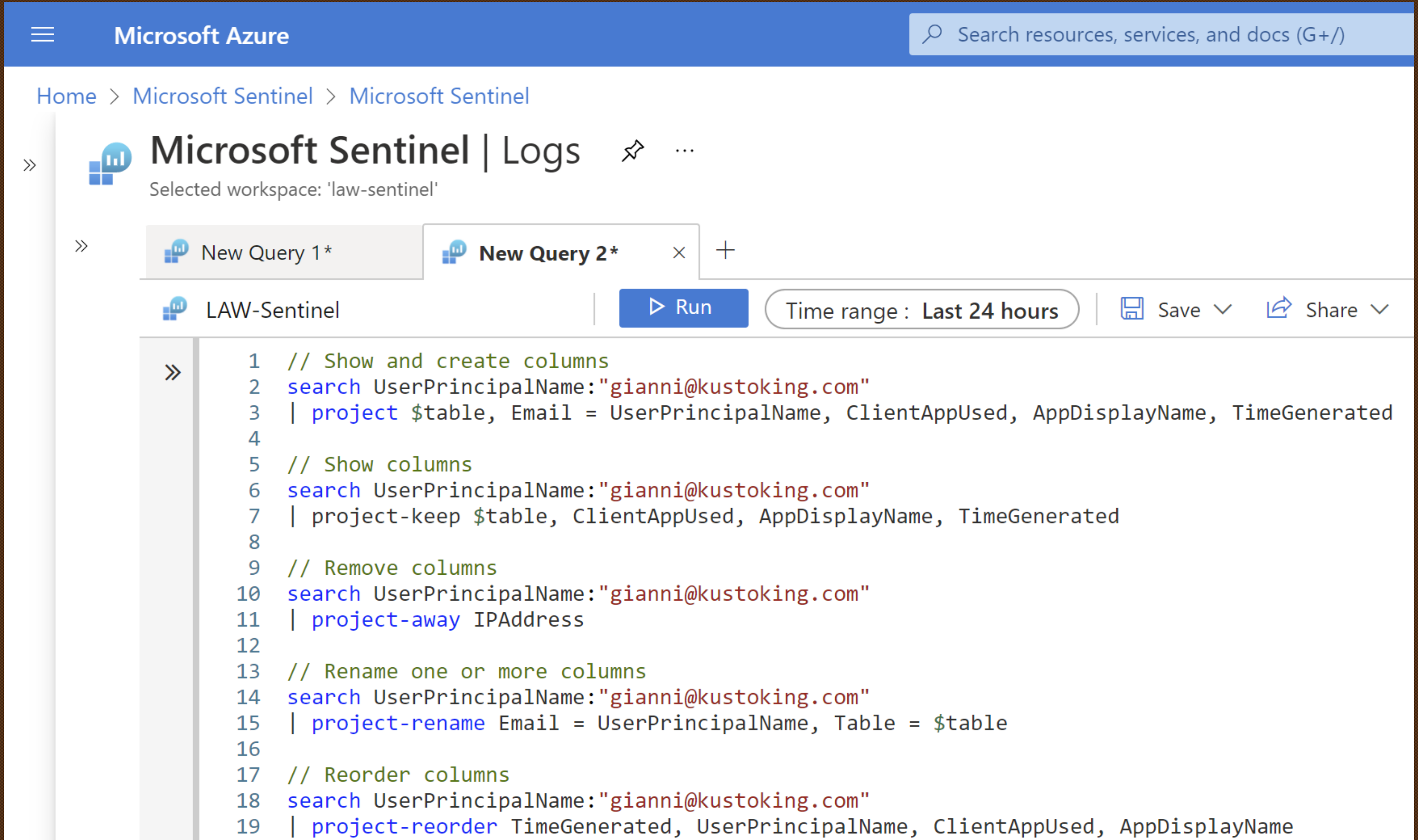
search



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-sentinel'
New Query 1 *
LAW-Sentinel
Run
Time range : Last 24 hours
Save
Share
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
LogManagement
Microsoft Sentinel

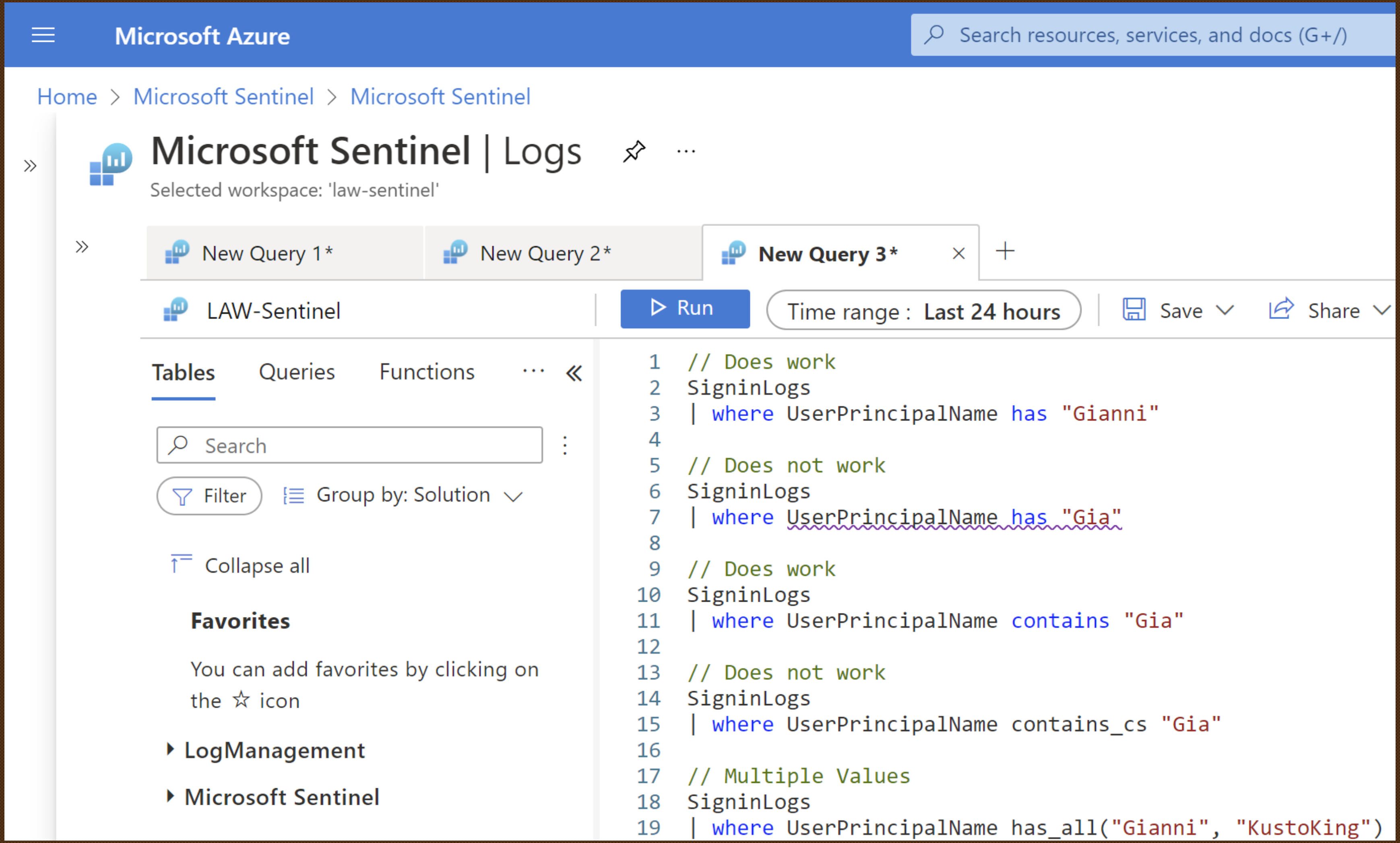
```
// contains
search "*kustoking*"

// has
search "kustoking"

// prefix
search "gianni*"

// suffix
search "*kustoking.com"

// search in tables
search in (OfficeActivity, SigninLogs, AAD*) "kustoking"

// search all tables with column
search UserPrincipalName:"gianni@kustoking.com"
```

project


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-sentinel'
New Query 1*
New Query 2*
LAW-Sentinel
Run
Time range : Last 24 hours
Save
Share

```
// Show and create columns
search UserPrincipalName:"gianni@kustoking.com"
| project $table, Email = UserPrincipalName, ClientAppUsed, AppDisplayName, TimeGenerated

// Show columns
search UserPrincipalName:"gianni@kustoking.com"
| project-keep $table, ClientAppUsed, AppDisplayName, TimeGenerated

// Remove columns
search UserPrincipalName:"gianni@kustoking.com"
| project-away IPAddress

// Rename one or more columns
search UserPrincipalName:"gianni@kustoking.com"
| project-rename Email = UserPrincipalName, Table = $table

// Reorder columns
search UserPrincipalName:"gianni@kustoking.com"
| project-reorder TimeGenerated, UserPrincipalName, ClientAppUsed, AppDisplayName
```

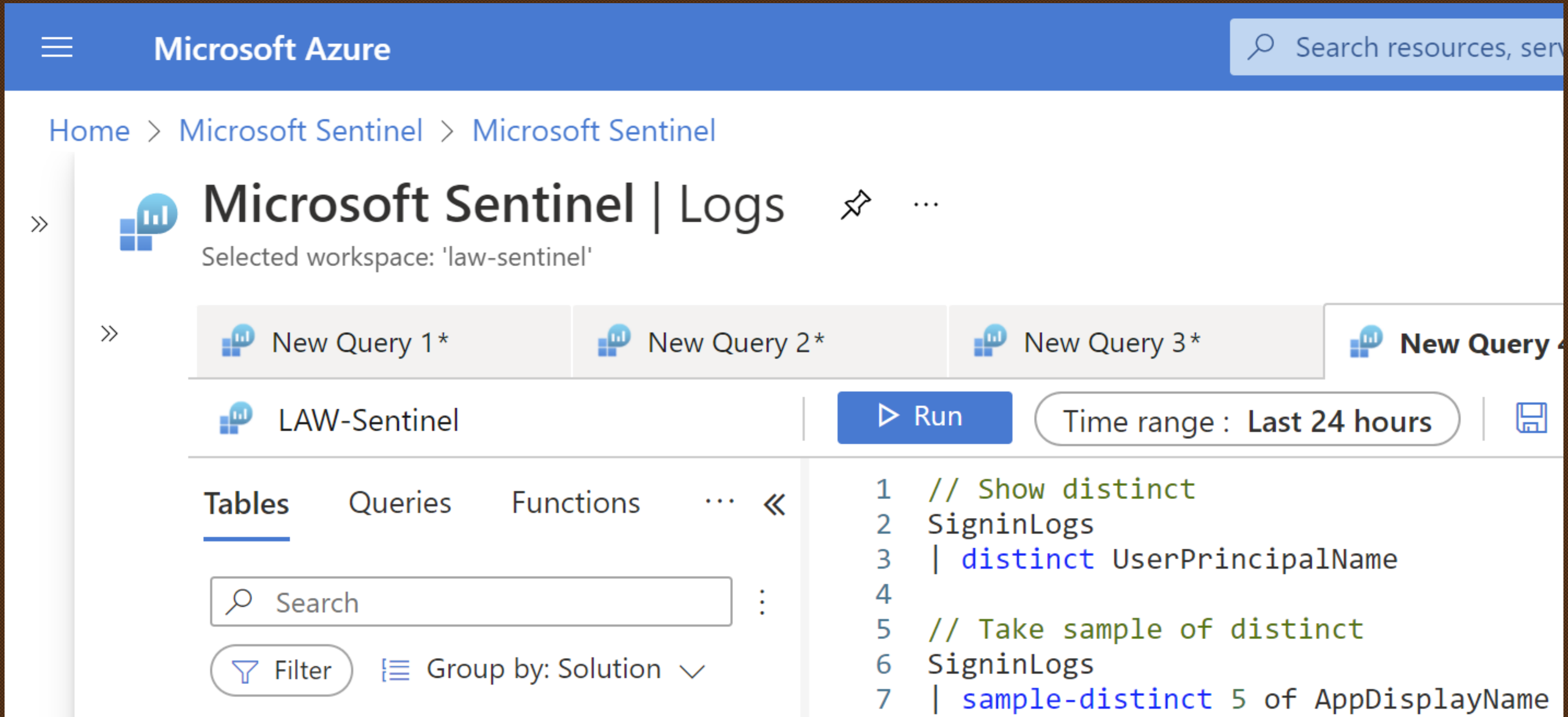
has <> contains



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-sentinel'
New Query 1*
New Query 2*
New Query 3*
LAW-Sentinel
Run
Time range : Last 24 hours
Save
Share
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon
LogManagement
Microsoft Sentinel

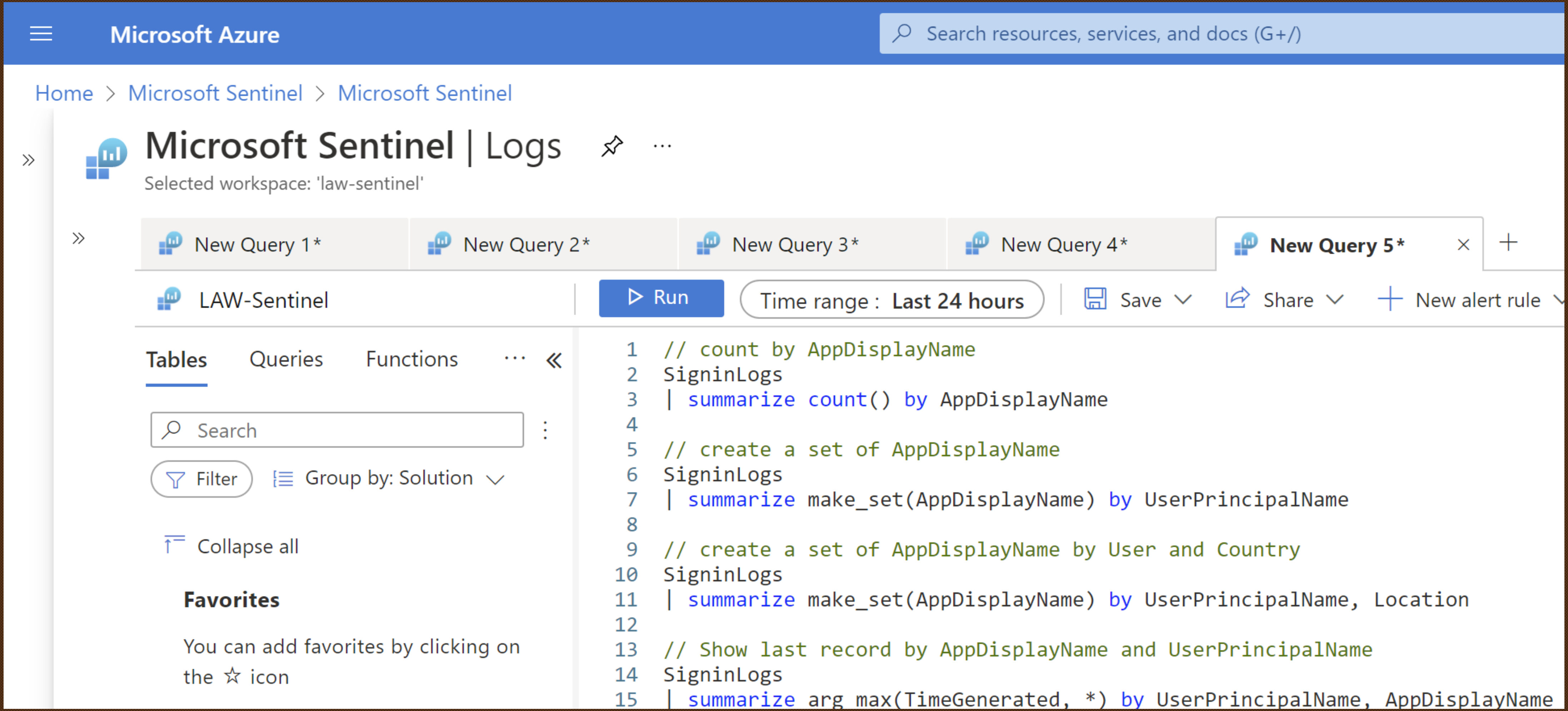
```
// Does work
SigninLogs
| where UserPrincipalName has "Gianni"

// Does not work
SigninLogs
| where UserPrincipalName has "Gia"

// Does work
SigninLogs
| where UserPrincipalName contains "Gia"

// Does not work
SigninLogs
| where UserPrincipalName contains_cs "Gia"

// Multiple Values
SigninLogs
| where UserPrincipalName has_all("Gianni", "KustoKing")
```

distinct



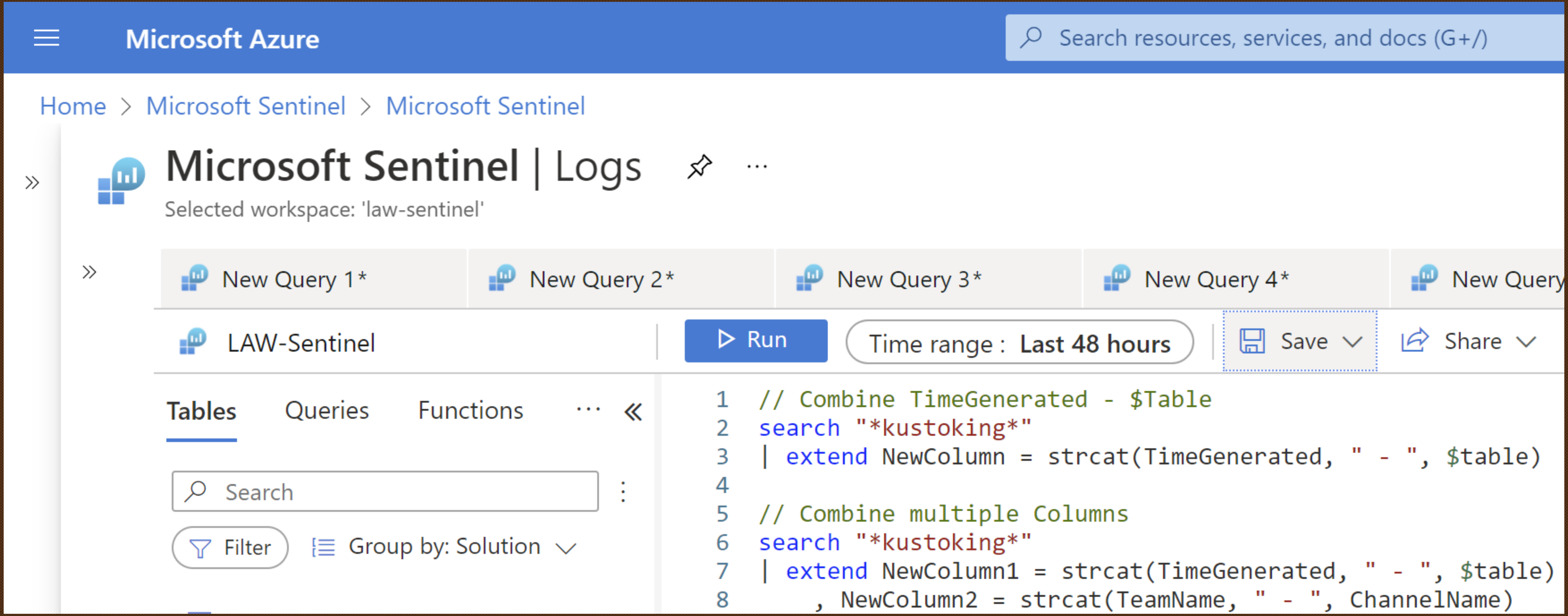
```
// Show distinct
SigninLogs
| distinct UserPrincipalName

// Take sample of distinct
SigninLogs
| sample-distinct 5 of AppDisplayName
```

summarize


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-sentinel'
New Query 1*
New Query 2*
New Query 3*
New Query 4*
New Query 5*
LAW-Sentinel
Run
Time range : Last 24 hours
Save
Share
New alert rule
Tables
Queries
Functions
Search
Filter
Group by: Solution
Collapse all
Favorites
You can add favorites by clicking on the ☆ icon

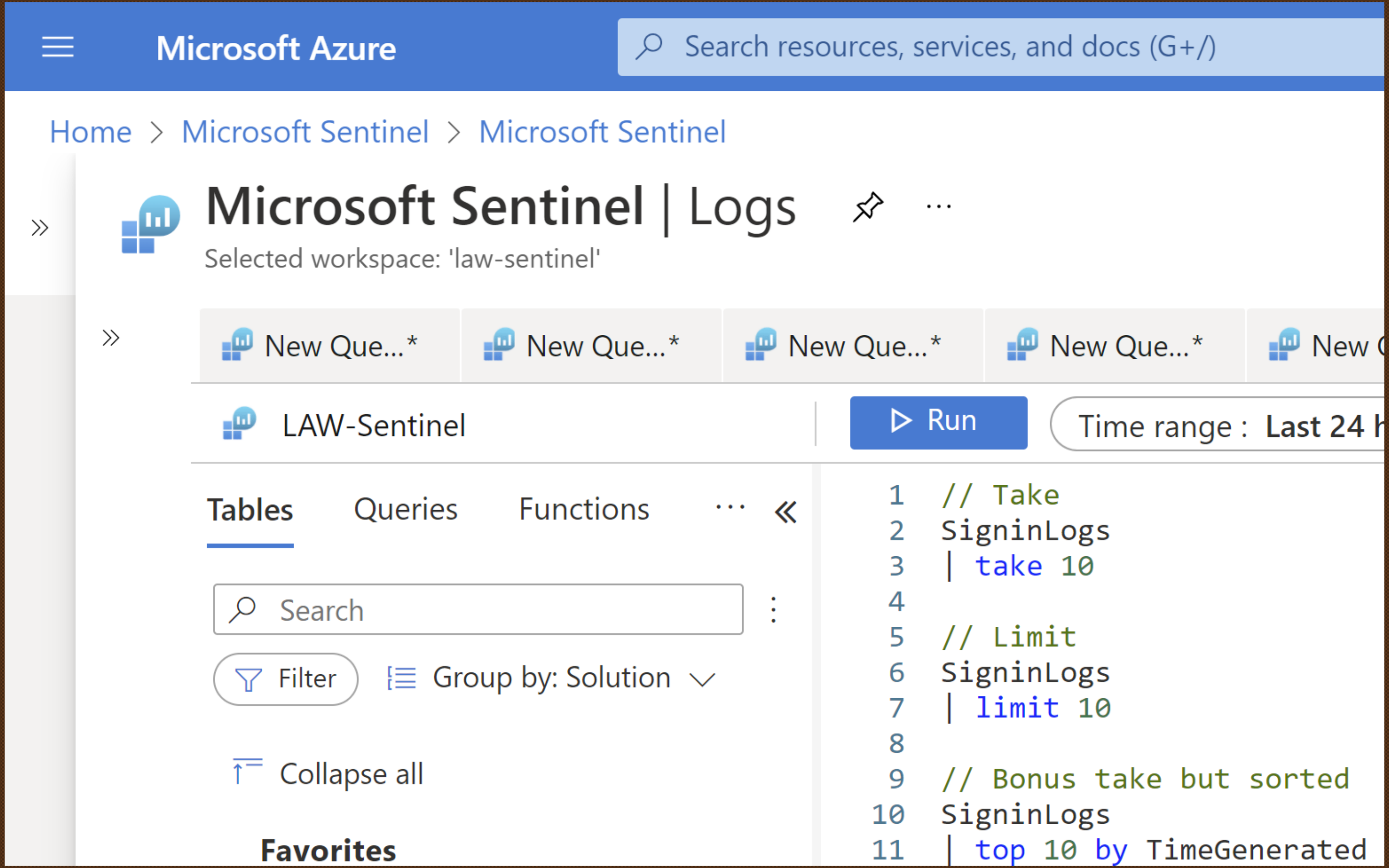
```
// count by AppDisplayName
SigninLogs
| summarize count() by AppDisplayName

// create a set of AppDisplayName
SigninLogs
| summarize make_set(AppDisplayName) by UserPrincipalName

// create a set of AppDisplayName by User and Country
SigninLogs
| summarize make_set(AppDisplayName) by UserPrincipalName, Location

// Show last record by AppDisplayName and UserPrincipalName
SigninLogs
| summarize arg_max(TimeGenerated, *) by UserPrincipalName, AppDisplayName
```

extend


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'law-sentinel'
New Query 1 *
New Query 2 *
New Query 3 *
New Query 4 *
New Query
LAW-Sentinel
Run
Time range : Last 48 hours
Save
Share
Tables
Queries
Functions
Search
Filter
Group by: Solution

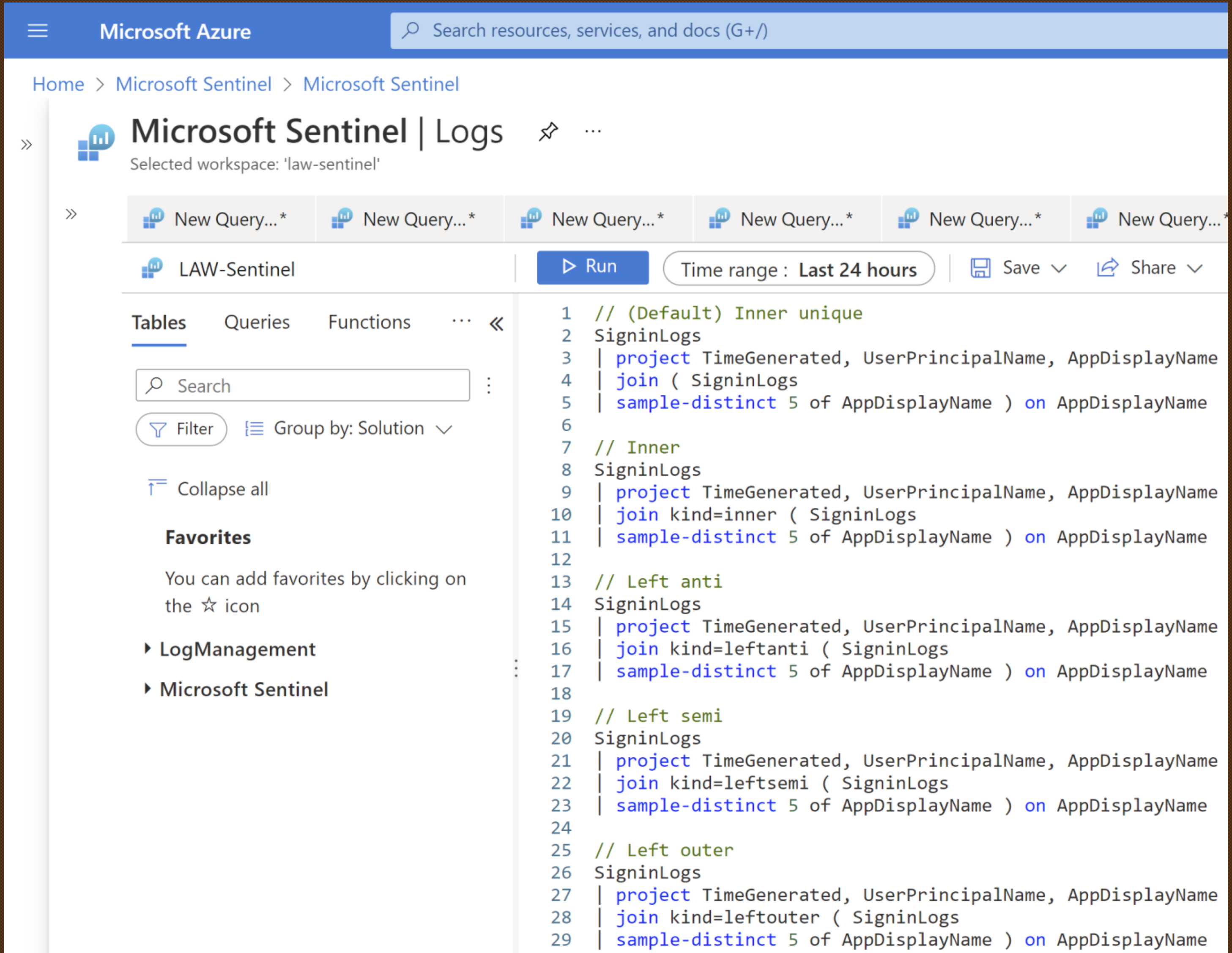
```
// Combine TimeGenerated - $Table
search "*kustoking*"
| extend NewColumn = strcat(TimeGenerated, " - ", $table)

// Combine multiple Columns
search "*kustoking*"
| extend NewColumn1 = strcat(TimeGenerated, " - ", $table)
    , NewColumn2 = strcat(TeamName, " - ", ChannelName)
```

take <> limit



```
// Take
SigninLogs
| take 10

// Limit
SigninLogs
| limit 10

// Bonus take but sorted
SigninLogs
| top 10 by TimeGenerated
```

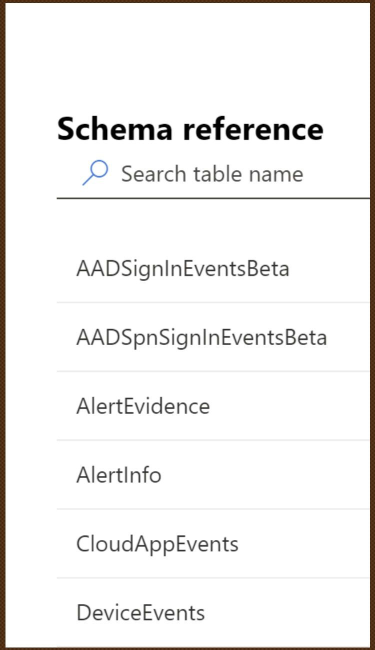
join



```
// (Default) Inner unique
SigninLogs
| project TimeGenerated, UserPrincipalName, AppDisplayName
| join ( SigninLogs
| sample-distinct 5 of AppDisplayName ) on AppDisplayName

// Inner
SigninLogs
| project TimeGenerated, UserPrincipalName, AppDisplayName
| join kind=inner ( SigninLogs
| sample-distinct 5 of AppDisplayName ) on AppDisplayName

// Left anti
SigninLogs
| project TimeGenerated, UserPrincipalName, AppDisplayName
| join kind=leftanti ( SigninLogs
| sample-distinct 5 of AppDisplayName ) on AppDisplayName

// Left semi
SigninLogs
| project TimeGenerated, UserPrincipalName, AppDisplayName
| join kind=leftsemi ( SigninLogs
| sample-distinct 5 of AppDisplayName ) on AppDisplayName

// Left outer
SigninLogs
| project TimeGenerated, UserPrincipalName, AppDisplayName
| join kind=leftouter ( SigninLogs
| sample-distinct 5 of AppDisplayName ) on AppDisplayName
```

How to find new things?

Microsoft Defender 365
Schema Reference
Microsoft Tech Docs


Schema reference

Search table name

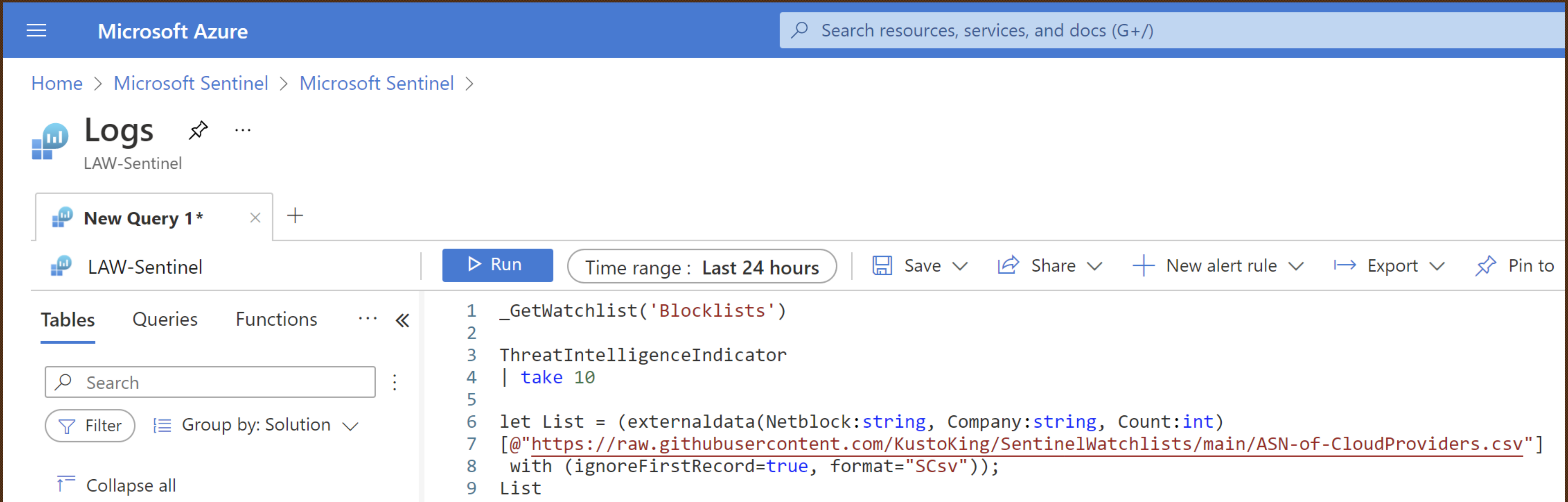
- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- AlertEvidence
- AlertInfo
- CloudAppEvents
- DeviceEvents

https://docs.microsoft.com/microsoft-365/security/defender/advanced-hunting-schema-tables

Working with IOCs

Microsoft 365 Defender
Microsoft Sentinel

Microsoft Sentinel



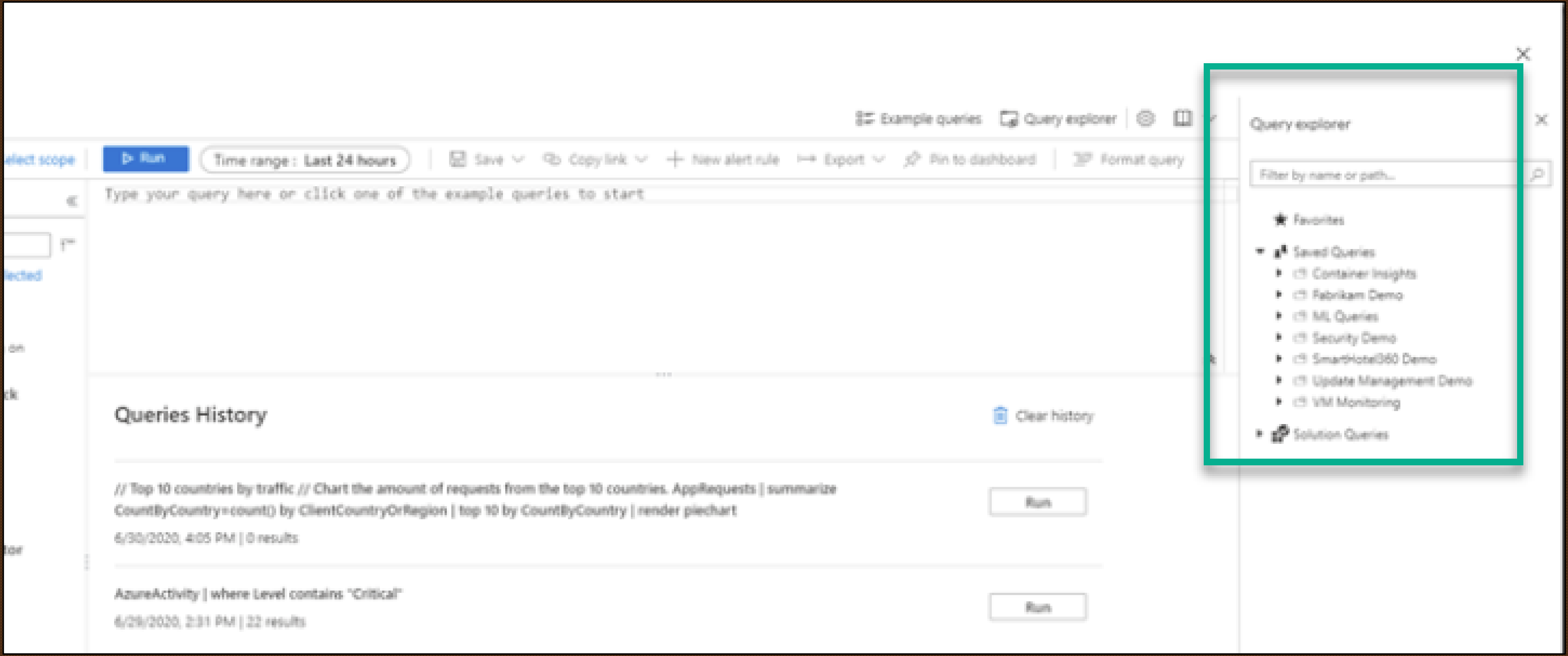
```
_GetWatchlist('Blocklists')

ThreatIntelligenceIndicator
| take 10

let List = (externaldata(Netblock:string, Company:string, Count:int)
[@"https://raw.githubusercontent.com/KustoKing/SentinelWatchlists/main/ASN-of-CloudProviders.csv"]
 with (ignoreFirstRecord=true, format="SCsv"));
List
```

Features worth Mentioning

Azure Query Packs

Advanced KQL for Microsoft Sentinel workbook

Previously in query explorer



Queries History

// Top 10 countries by traffic // Chart the amount of requests from the top 10 countries. AppRequests | summarize CountByCountry=count() by ClientCountryOrRegion | top 10 by CountByCountry | render piechart

6/30/2020, 4:05 PM | 0 results

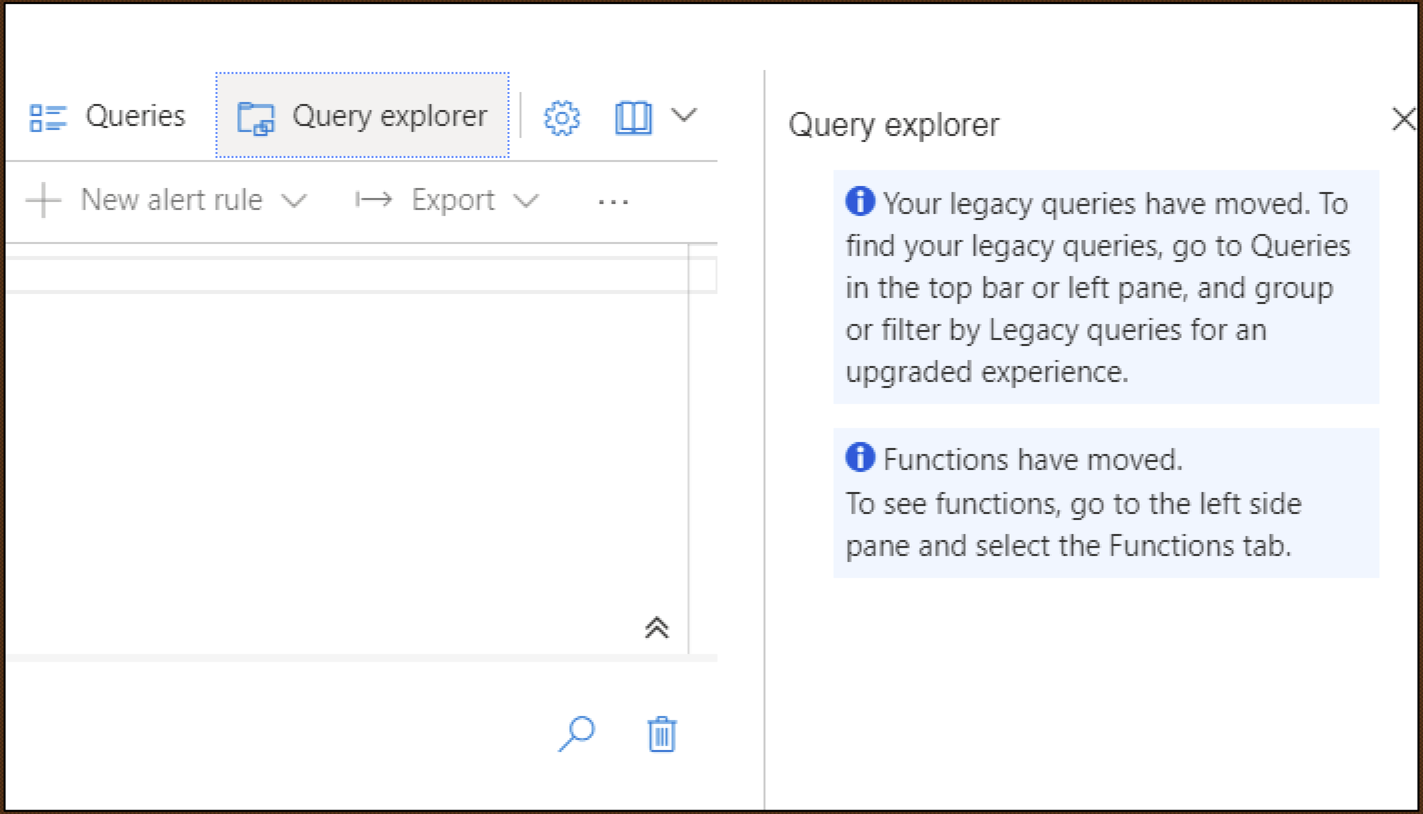
Run

AzureActivity | where Level contains "Critical"

6/29/2020, 2:31 PM | 22 results

Run

Now moved

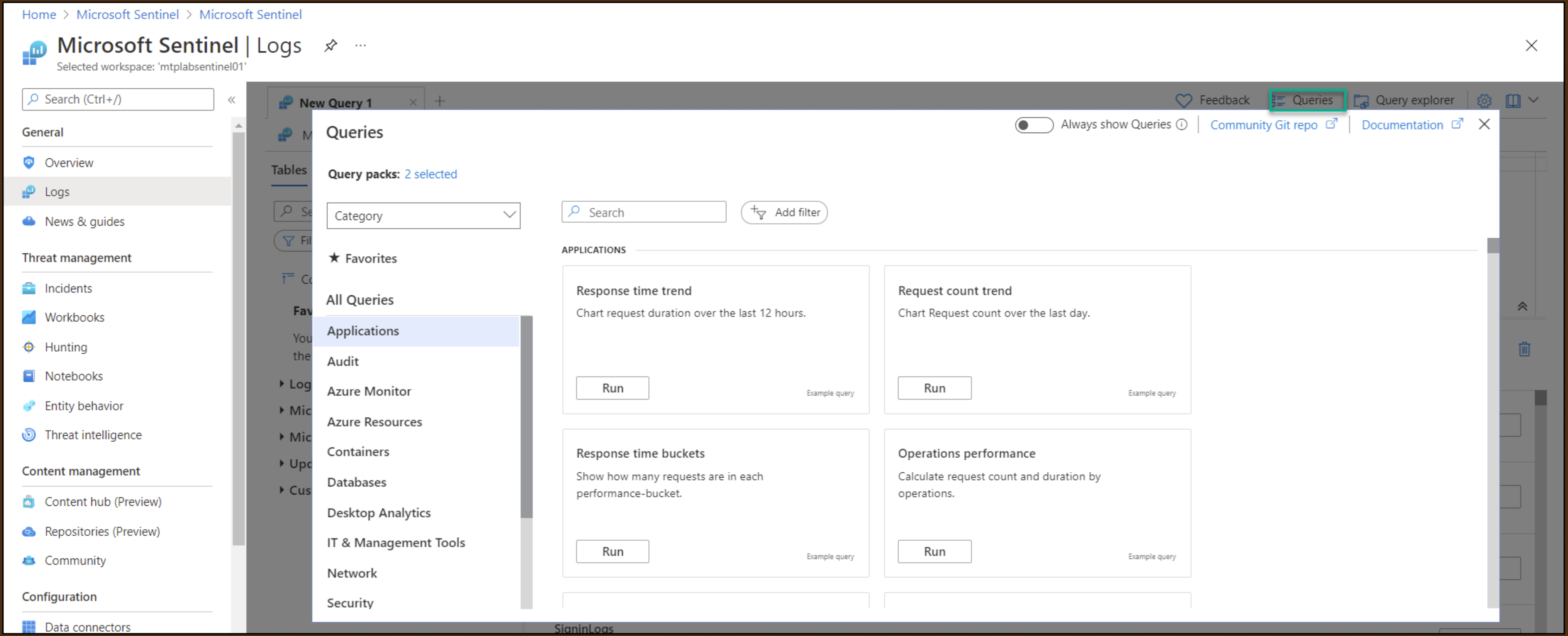


Query explorer

Your legacy queries have moved. To find your legacy queries, go to Queries in the top bar or left pane, and group or filter by Legacy queries for an upgraded experience.

Functions have moved.
To see functions, go to the left side pane and select the Functions tab.

To Queries



Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Logs

Selected workspace: 'mtplabsentinel01'

Queries

Query packs: 2 selected

Response time trend
Chart request duration over the last 12 hours.

Request count trend
Chart Request count over the last day.

Response time buckets
Show how many requests are in each performance-bucket.

Operations performance
Calculate request count and duration by operations.

Log Analytics query packs
A log Analytics query pack is a container for queries, designed to store and manage queries in an effective way.

Query Packs are ARM objects - allowing users to granularly control various aspects of the query pack including permissions, where it is stored, deployment etc.

Query packs exist at the subscription level - meaning your queries stored in a Query Pack are **available to your users across Log Analytics resources and workspaces** - eliminating silos. Save your query once, and use it everywhere in Log Analytics.

Query packs are designed as ARM objects

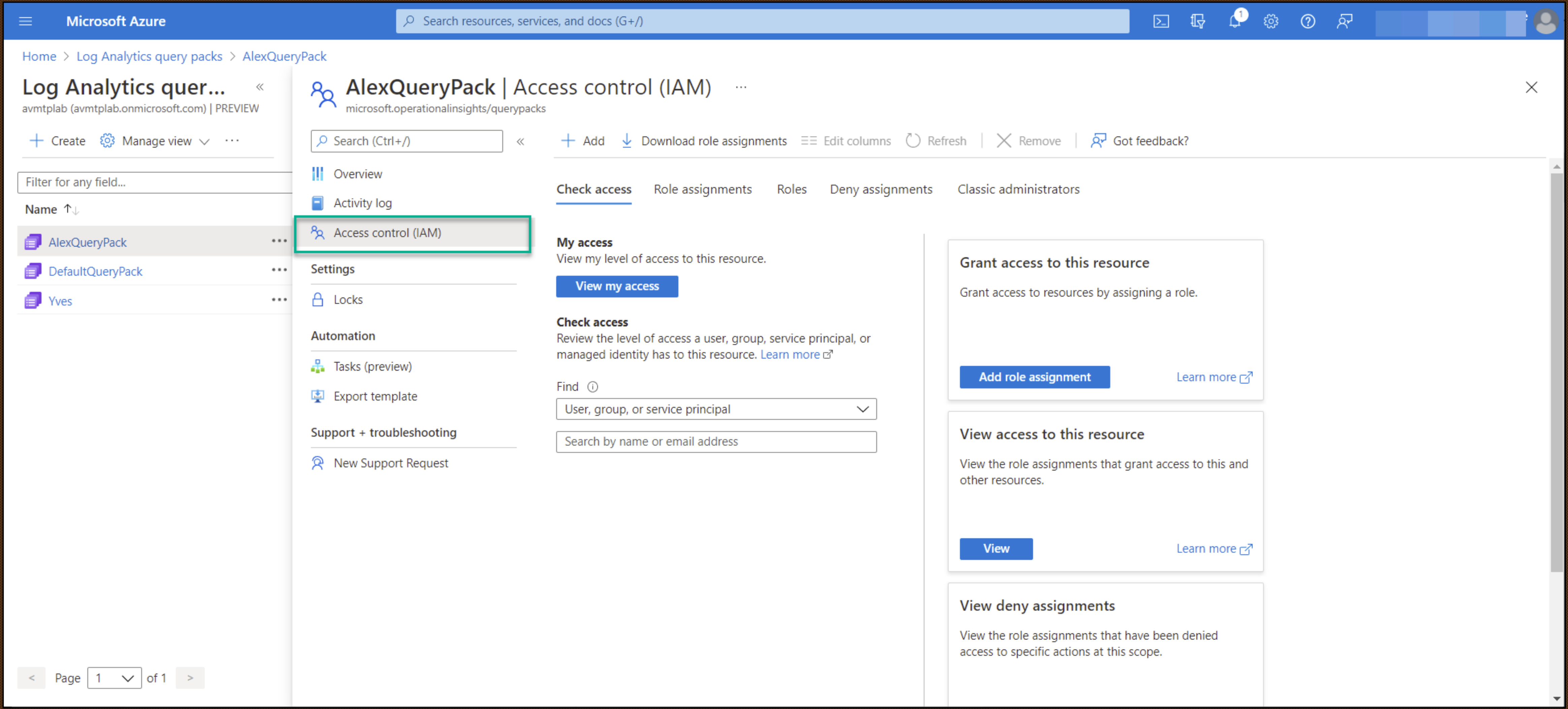
RBAC at query pack level

Deploy as code

Export Query Pack

Manage from API

RBAC at query pack level



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Log Analytics query packs > AlexQueryPack

Log Analytics quer...

avmtplab (avmtplab.onmicrosoft.com) | PREVIEW

+ Create   Manage view   ...

Filter for any field...

Name ↑↓

- AlexQueryPack
- DefaultQueryPack
- Yves

< Page 1 of 1 >

AlexQueryPack | Access control (IAM) ...

microsoft.operationalinsights/querypacks

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)

Settings

- Locks

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- New Support Request

+ Add   Download role assignments   Edit columns   Refresh   Remove   Got feedback?

Check access   Role assignments   Roles   Deny assignments   Classic administrators

My access

View my level of access to this resource.

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find

User, group, or service principal

Search by name or email address

Grant access to this resource

Grant access to resources by assigning a role.

Add role assignment   Learn more

View access to this resource

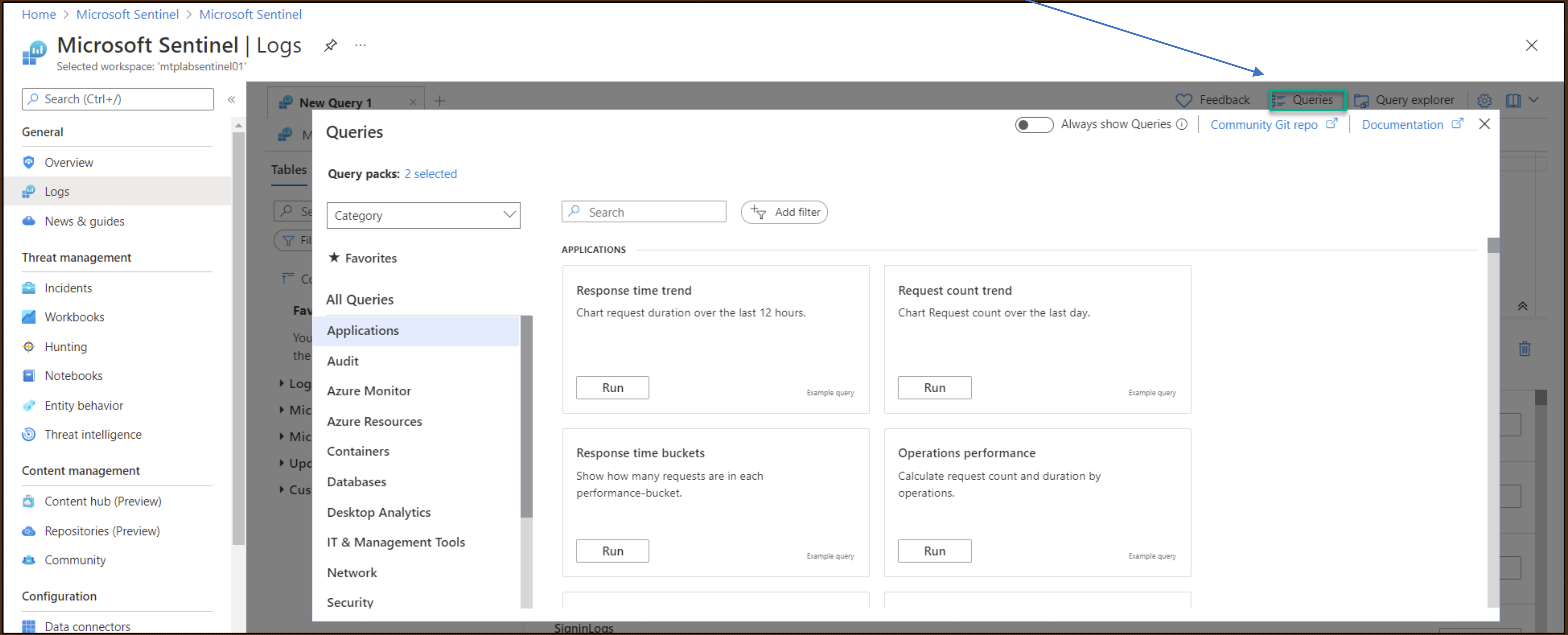
View the role assignments that grant access to this and other resources.

View   Learn more

View deny assignments

View the role assignments that have been denied access to specific actions at this scope.

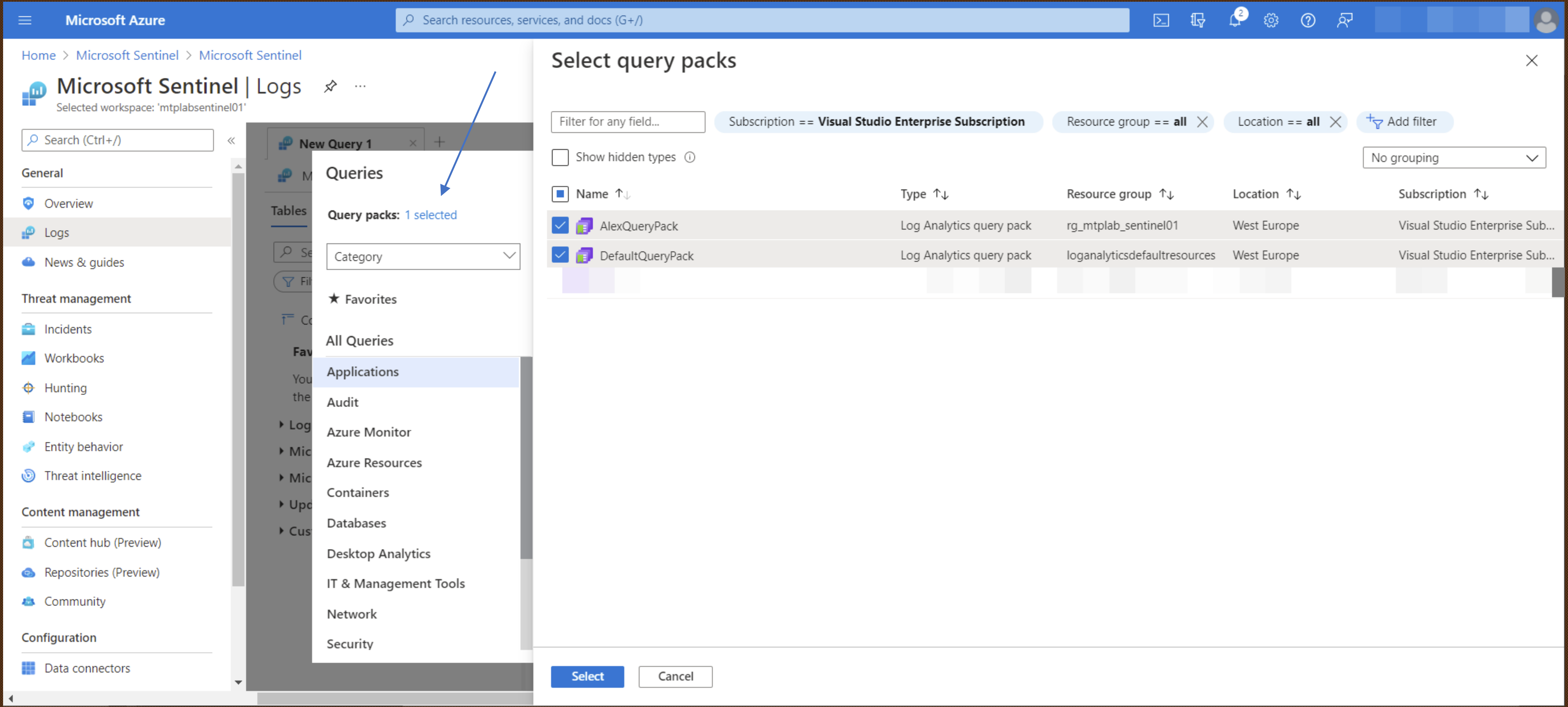
Access Query Packs



Features worth Mentioning

Session 1 | Getting started

Use multiple query packs



Query packs: 1 selected

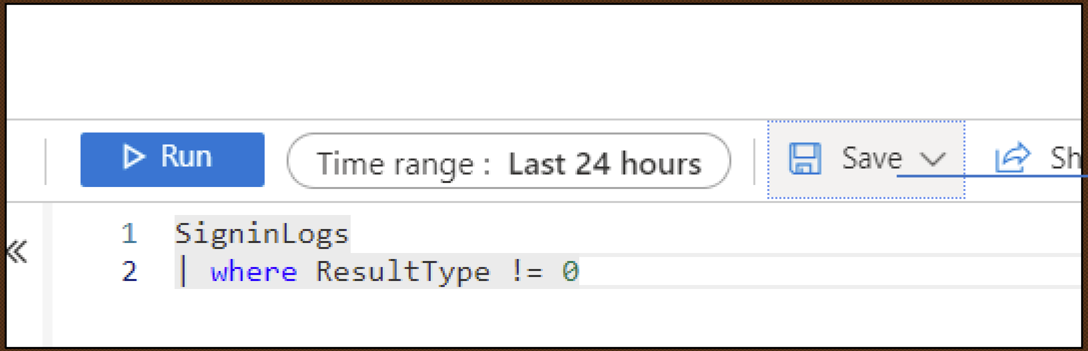
Select query packs

Subscription == **Visual Studio Enterprise Subscription** | Resource group == **all** | Location == **all**

☐ Show hidden types

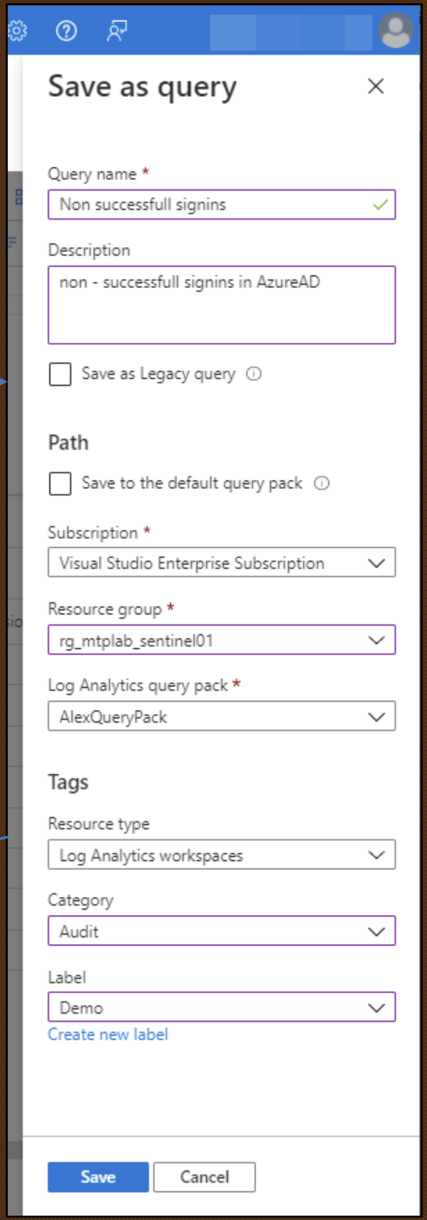
	Name	Type	Resource group	Location	Subscription
☑	AlexQueryPack	Log Analytics query pack	rg_mtplab_sentinel01	West Europe	Visual Studio Enterprise Sub...
☑	DefaultQueryPack	Log Analytics query pack	loganalyticsdefaultresources	West Europe	Visual Studio Enterprise Sub...

Save a query to a pack



Time range : Last 24 hours

```
SigninLogs
| where ResultType != 0
```



Save as query

Query name * Non successfull signins

Description: non - successfull signins in AzureAD

□ Save as Legacy query

Path

□ Save to the default query pack

Subscription * Visual Studio Enterprise Subscription

Resource group * rg_mtplab_sentinel01

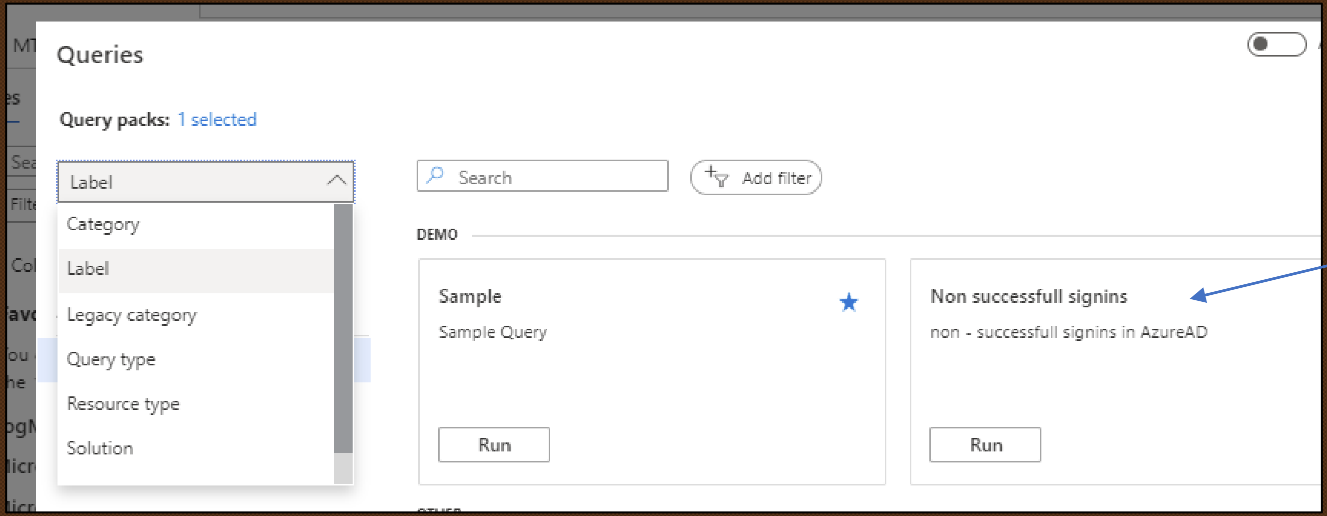
Log Analytics query pack * AlexQueryPack

Tags

Resource type: Log Analytics workspaces

Category: Audit

Label: Demo



Queries

Query packs: 1 selected

DEMO

Sample Sample Query	Non successfull signins non - successfull signins in AzureAD

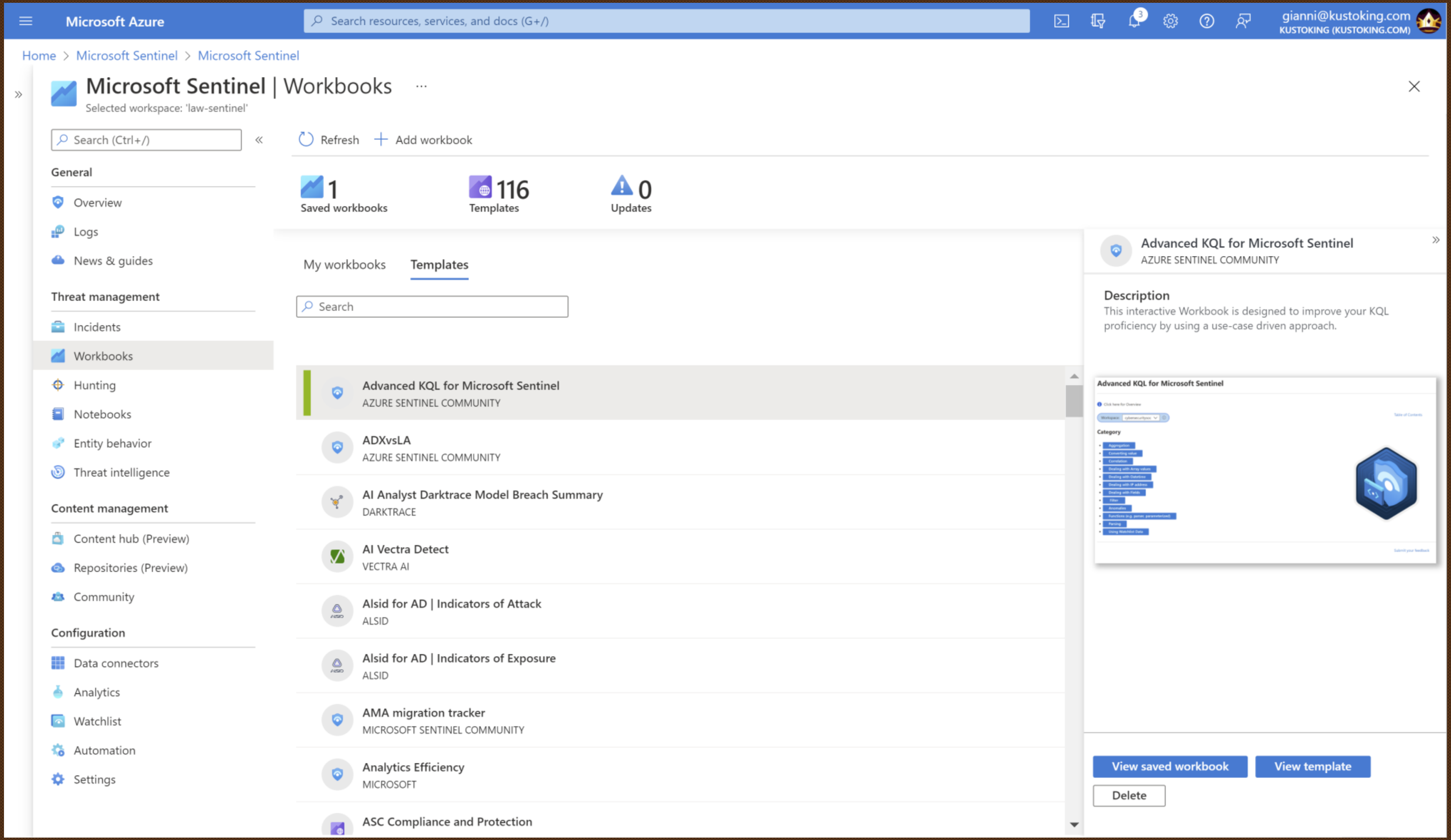
Recomended reads

https://techcommunity.microsoft.com/t5/azure-monitor-blog/log-analytics-query-packs/ba-p/2314721

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/queries

https://azure.microsoft.com/en-us/updates/saved-searches-functionality-is-moving-to-query-explorer/

Advanced KQL for Microsoft Sentinel workbook



Microsoft Azure
Search resources, services, and docs (G+/)
gianni@kustoking.com
KUSTOKING (KUSTOKING.COM)
Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Workbooks

Selected workspace: 'law-sentinel'

1 Saved workbooks

116 Templates

0 Updates

Advanced KQL for Microsoft Sentinel	AZURE SENTINEL COMMUNITY
ADXvsLA	AZURE SENTINEL COMMUNITY
AI Analyst Darktrace Model Breach Summary	DARKTRACE
AI Vectra Detect	VECTRA AI
Alsid for AD | Indicators of Attack	ALSID
Alsid for AD | Indicators of Exposure	ALSID
AMA migration tracker	MICROSOFT SENTINEL COMMUNITY
Analytics Efficiency	MICROSOFT
ASC Compliance and Protection	

Advanced KQL for Microsoft Sentinel

AZURE SENTINEL COMMUNITY

Description

This interactive Workbook is designed to improve your KQL proficiency by using a use-case driven approach.

Features worth Mentioning

And now we present this week's guest.

What did you do with KQL this month?

KQL Challenge of the month

Questions?

Thanks for attending

KQL|Cafe