geekmania

geekmania

Introduction to KQL

Alex Verboon | baseVISION AG

MVP Microsoft® Most Valuable Professional

GSEC

baseVISION

SECURE & MODERN WORKPLACE

- **Alex Verboon**
  CTO - Principal Cyber Security Consultant

- **Contact Me**

https://twitter.com/alexverboon

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

GitHub https://github.com/alexverboon

https://www.verboon.info/

geekmania

baseVISION

SECURE & MODERN WORKPLACE

Microsoft | Schweiz
Partner of the Year 2022
Security

Microsoft | Schweiz
Partner of the Year 2021
Security

Microsoft | Schweiz
Partner of the Year 2018
Empower Employees

Microsoft | Schweiz
Partner of the Year 2016
Cloud Innovation: Public Sector

Great Place To Work®
Certified
APR 2022-APR 2023
CH
TM

Microsoft
Solutions Partner
Security

Specialist
Identity and Access Management
Threat Protection

Microsoft
Solutions Partner
Modern Work

Specialist
Modernize Endpoints

Microsoft
Solutions Partner
Infrastructure
Azure

kununu
TOP COMPANY
www.kununu.com
VON MITARBEITERN EMPFOHLEN!

ISO/IEC 27001:2013
BUREAU VERITAS
Certification

BUREAU VERITAS
1828

UKAS
MANAGEMENT SYSTEMS
0008

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

geekmania

Why Learn KQL?

Why you should learn KQL

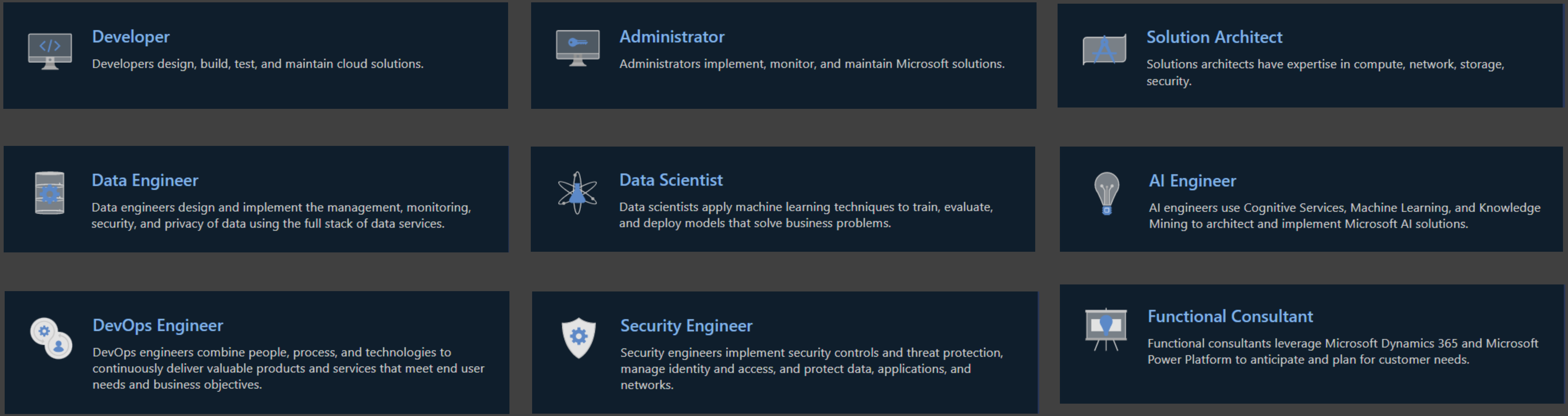
IT Pro Toolbox

Skills that help you mastering your daily tasks as an IT Pro

1990	2000	2010	2023
Windows Batch Scripting	VB Script	PowerShell	**KQL**

geekmania

Why you should learn KQL



Developer

Developers design, build, test, and maintain cloud solutions.

Administrator

Administrators implement, monitor, and maintain Microsoft solutions.

Solution Architect

Solutions architects have expertise in compute, network, storage, security.

Data Engineer

Data engineers design and implement the management, monitoring, security, and privacy of data using the full stack of data services.

Data Scientist

Data scientists apply machine learning techniques to train, evaluate, and deploy models that solve business problems.

AI Engineer

AI engineers use Cognitive Services, Machine Learning, and Knowledge Mining to architect and implement Microsoft AI solutions.

DevOps Engineer

DevOps engineers combine people, process, and technologies to continuously deliver valuable products and services that meet end user needs and business objectives.

Security Engineer

Security engineers implement security controls and threat protection, manage identity and access, and protect data, applications, and networks.

Functional Consultant

Functional consultants leverage Microsoft Dynamics 365 and Microsoft Power Platform to anticipate and plan for customer needs.

No matter what IT career path you pursue, you’ll meet **KQL**

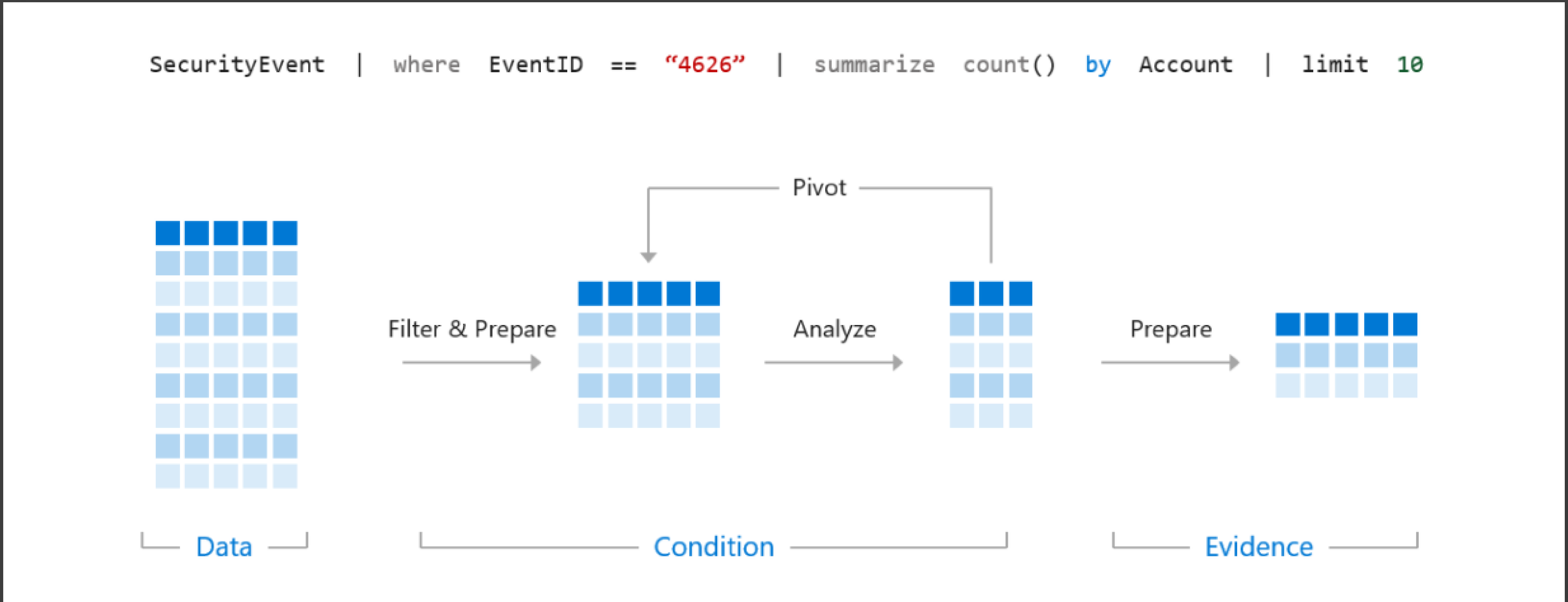
geekmania

Where to use KQL?

- Azure Monitor
- Azure Log Analytics
- Azure Data Explorer
- Azure Resource Graph
- Microsoft Sentinel
- Microsoft 365 Defender
- Microsoft Endpoint Manager (Configuration Manager & Intune)
- Microsoft Purview
- Azure Application Insights

KQL – What is a KQL Query?

A Kusto query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model that is easy to read, author, and automate. Kusto queries are made of one or more query statements.



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

geekmania

KQL

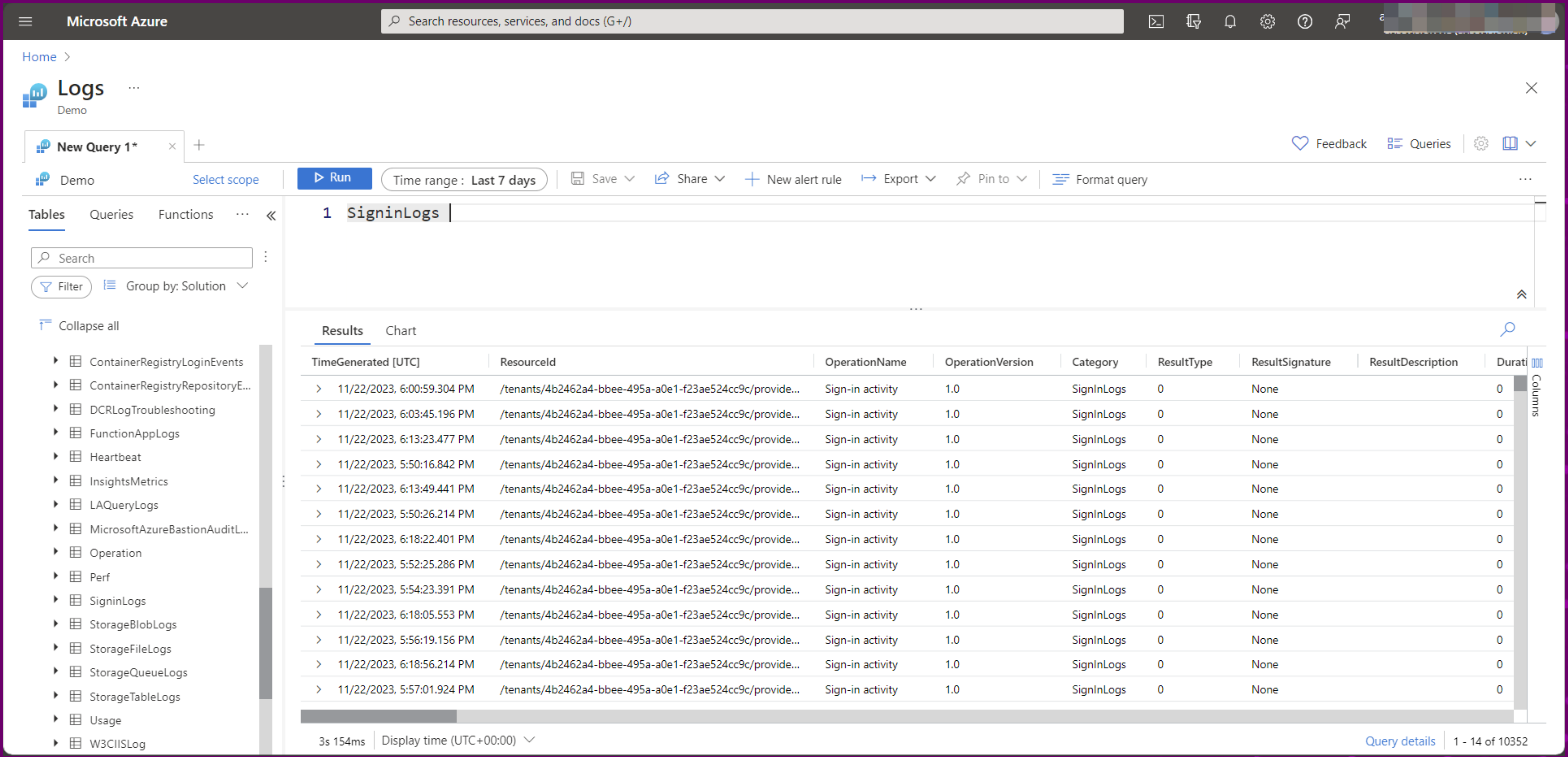
- Demo Environments
- Setup Your Own Environment

Log Analytics Demo Environment

https://portal.azure.com/#blade/Microsoft_Azure_Monitoring_Logs/DemoLogsBlade

FREE OF CHARGE!

geekmania



- ContainerRegistryLoginEvents
- ContainerRegistryRepositoryE...
- DCRLogTroubleshooting
- FunctionAppLogs
- Heartbeat
- InsightsMetrics
- LAQueryLogs
- MicrosoftAzureBastionAuditL...
- Operation
- Perf
- SigninLogs
- StorageBlobLogs
- StorageFileLogs
- StorageQueueLogs
- StorageTableLogs
- Usage
- W3CIISLog

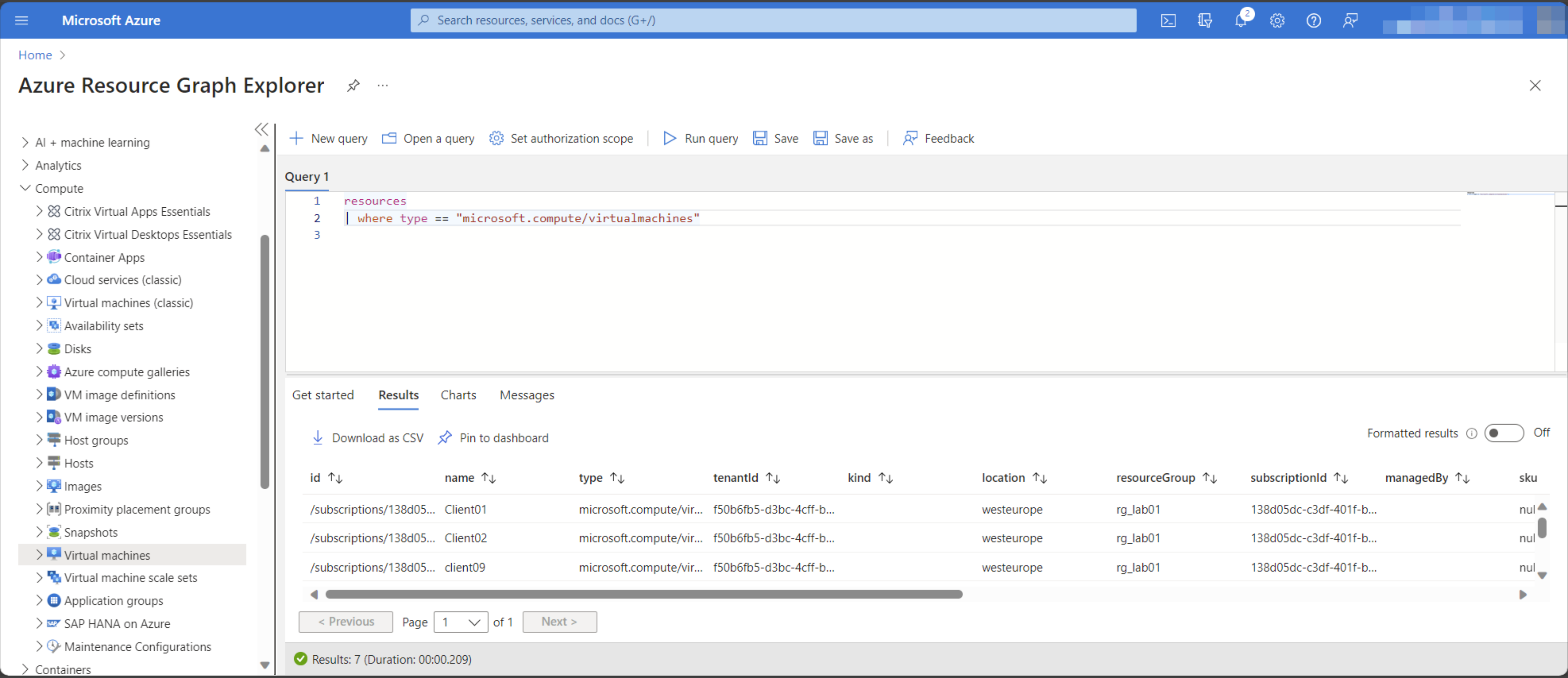
```
SigninLogs
```

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType	ResultSignature	ResultDescription	Durati
11/22/2023, 6:00:59.304 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:03:45.196 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:13:23.477 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:50:16.842 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:13:49.441 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:50:26.214 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:18:22.401 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:52:25.286 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:54:23.391 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:18:05.553 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:56:19.156 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 6:18:56.214 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0
11/22/2023, 5:57:01.924 PM	/tenants/4b2462a4-bbee-495a-a0e1-f23ae524cc9c/provide...	Sign-in activity	1.0	SignInLogs	0	None		0

3s 154ms | Display time (UTC+00:00) | Query details | 1 - 14 of 10352

geekmania

Azure Graph Explorer



```
resources
| where type == "microsoft.compute/virtualmachines"
```

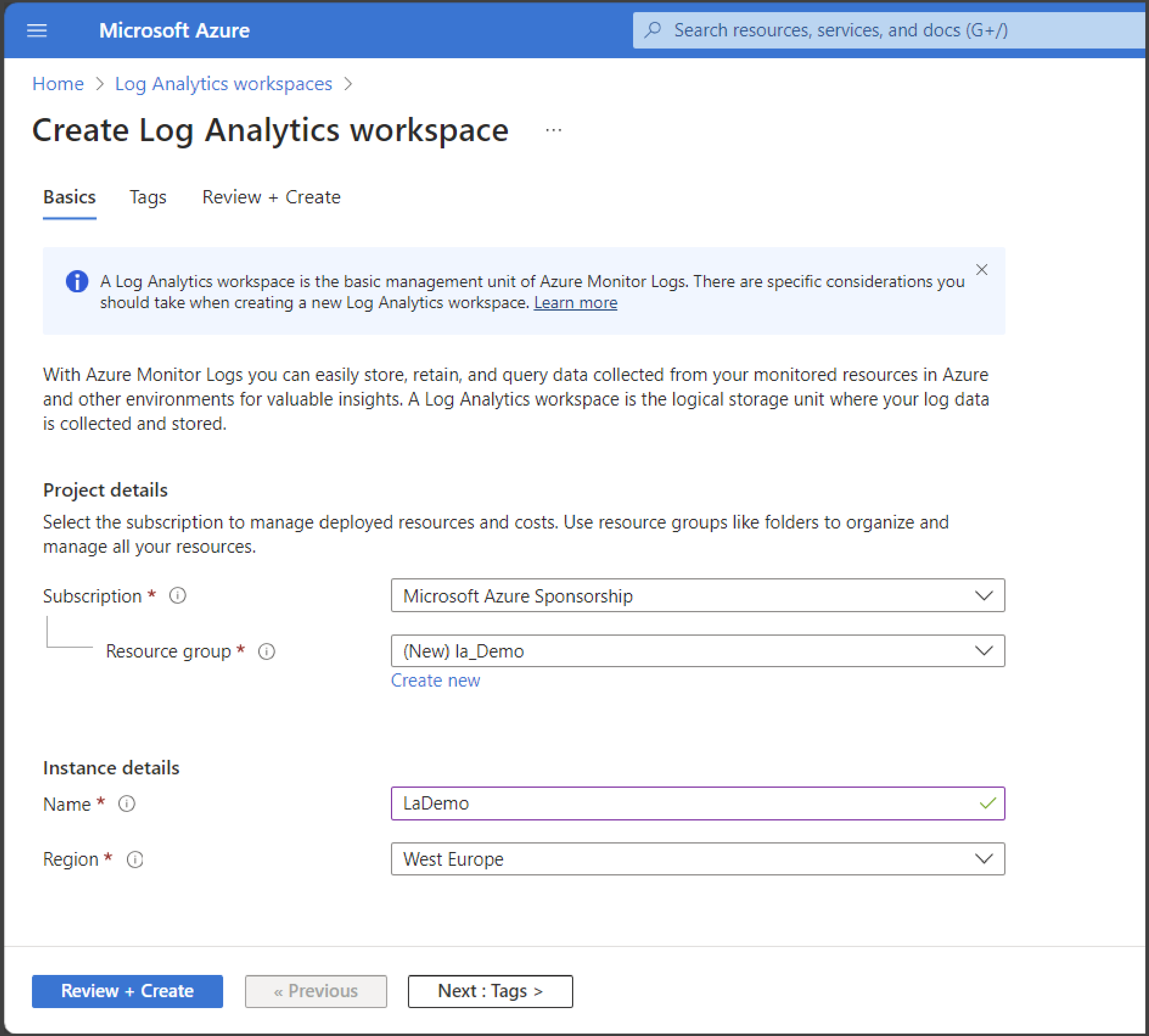
id	name	type	tenantId	kind	location	resourceGroup	subscriptionId	managedBy	sku
/subscriptions/138d05...	Client01	microsoft.compute/vir...	f50b6fb5-d3bc-4cff-b...		westeurope	rg_lab01	138d05dc-c3df-401f-b...		nul
/subscriptions/138d05...	Client02	microsoft.compute/vir...	f50b6fb5-d3bc-4cff-b...		westeurope	rg_lab01	138d05dc-c3df-401f-b...		nul
/subscriptions/138d05...	client09	microsoft.compute/vir...	f50b6fb5-d3bc-4cff-b...		westeurope	rg_lab01	138d05dc-c3df-401f-b...		nul

Results: 7 (Duration: 00:00.209)

Setup your own Environment

geekmania

Deploy your Log Analytics Workspace



Home > Log Analytics workspaces >

Create Log Analytics workspace ...

Basics | Tags | Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Azure Sponsorship

Resource group * : (New) la_Demo

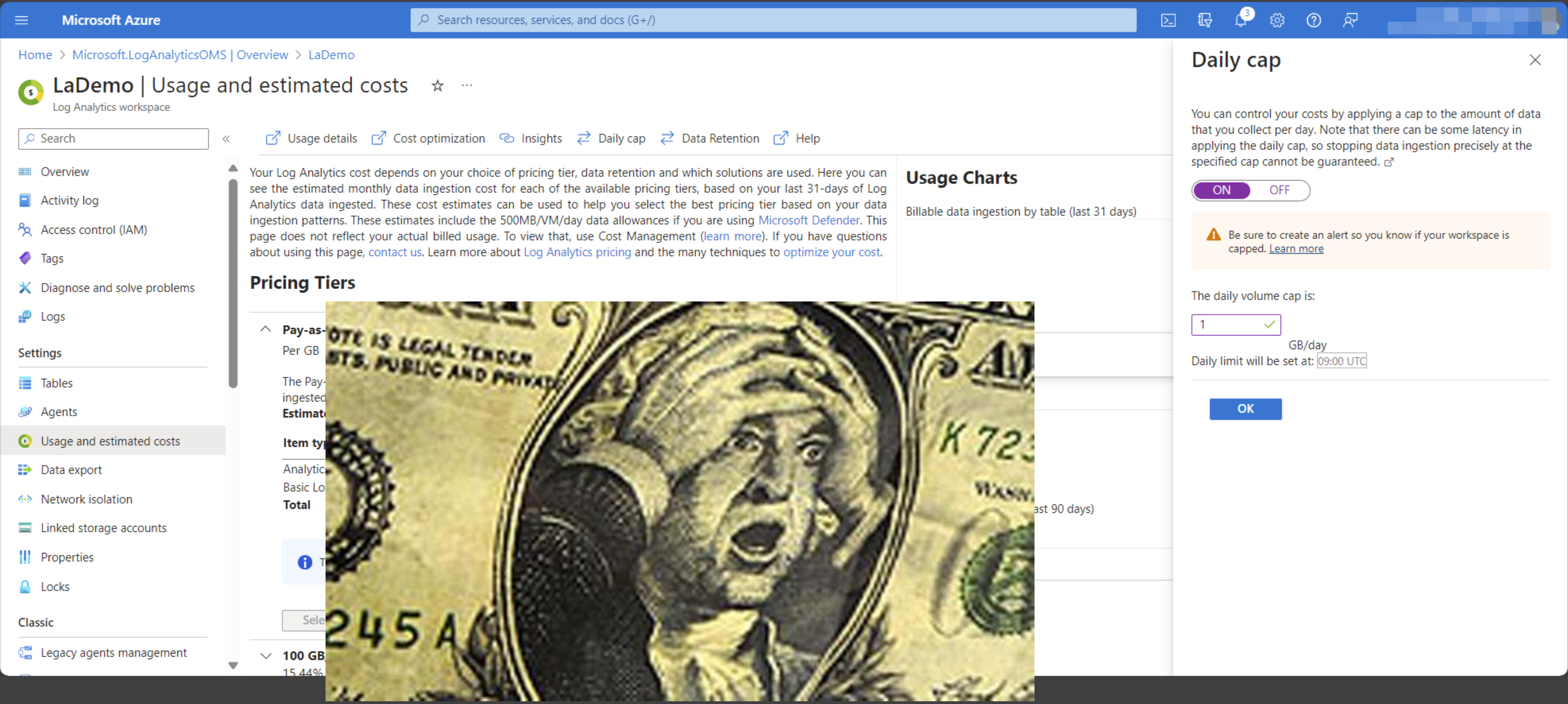
Create new

Instance details

Name * : LaDemo ✓

Region * : West Europe

Configure Daily Cap



Home > Microsoft.LogAnalyticsOMS | Overview > LaDemo

LaDemo | Usage and estimated costs

Log Analytics workspace

Search

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

Settings

- Tables
- Agents
- Usage and estimated costs
- Data export
- Network isolation
- Linked storage accounts
- Properties
- Locks

Classic

- Legacy agents management

Usage details | Cost optimization | Insights | Daily cap | Data Retention | Help

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly data ingestion cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Microsoft Defender. This page does not reflect your actual billed usage. To view that, use Cost Management (learn more). If you have questions about using this page, contact us. Learn more about Log Analytics pricing and the many techniques to optimize your cost.

Pricing Tiers

Pay-as-

Per GB

The Pay-

ingested

Estimat

Item ty

Analytic

Basic Lo

Total

Sele

100 GB

15.44%

Usage Charts

Billable data ingestion by table (last 31 days)

ast 90 days)

Daily cap

You can control your costs by applying a cap to the amount of data that you collect per day. Note that there can be some latency in applying the daily cap, so stopping data ingestion precisely at the specified cap cannot be guaranteed.

[✓ ON] OFF

⚠ Be sure to create an alert so you know if your workspace is capped. Learn more

The daily volume cap is:

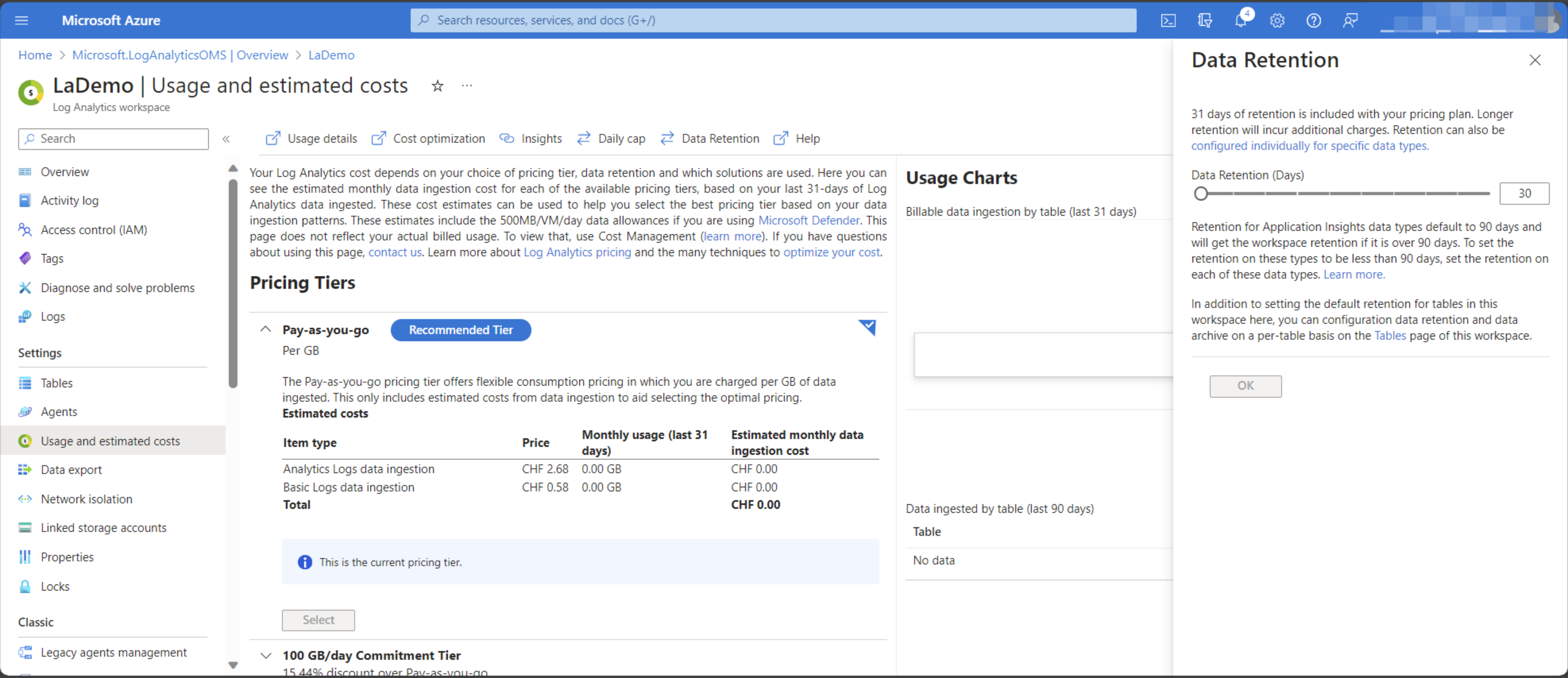
1 ✓ GB/day

Daily limit will be set at: 09:00 UTC

OK

geekmania

Configure Retention Period



Home > Microsoft.LogAnalyticsOMS | Overview > LaDemo

LaDemo | Usage and estimated costs

Log Analytics workspace

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly data ingestion cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Microsoft Defender. This page does not reflect your actual billed usage. To view that, use Cost Management (learn more). If you have questions about using this page, contact us. Learn more about Log Analytics pricing and the many techniques to optimize your cost.

Pricing Tiers

Pay-as-you-go Recommended Tier

Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. This only includes estimated costs from data ingestion to aid selecting the optimal pricing.

Estimated costs

Item type	Price	Monthly usage (last 31 days)	Estimated monthly data ingestion cost
Analytics Logs data ingestion	CHF 2.68	0.00 GB	CHF 0.00
Basic Logs data ingestion	CHF 0.58	0.00 GB	CHF 0.00
Total			**CHF 0.00**

This is the current pricing tier.

100 GB/day Commitment Tier

15.44% discount over Pay-as-you-go

Usage Charts

Billable data ingestion by table (last 31 days)

Data ingested by table (last 90 days)

Table
No data

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be configured individually for specific data types.

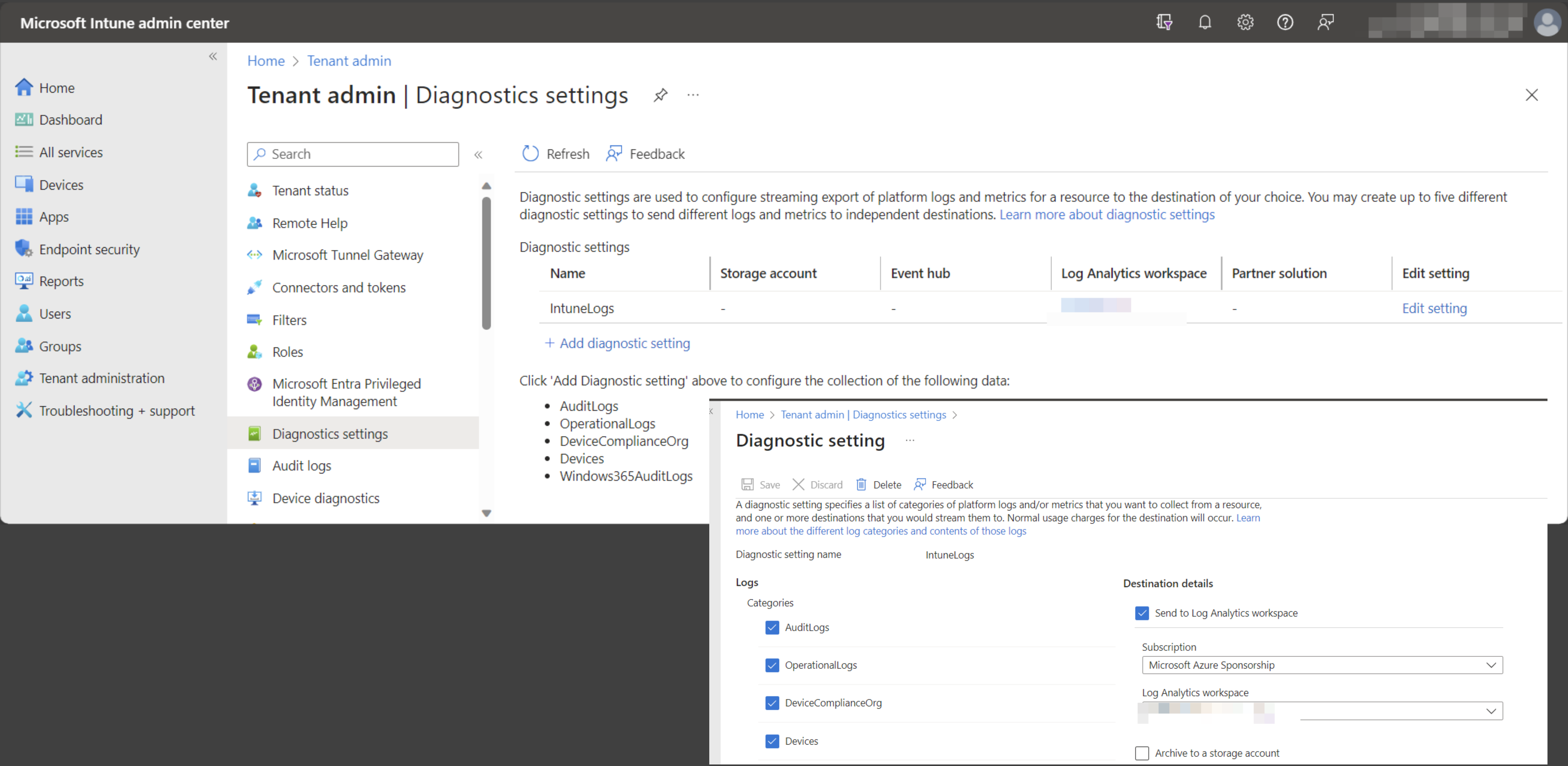
Data Retention (Days): 30

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. Learn more.

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the Tables page of this workspace.

geekmania

Bring your Intune Logs into Log Analytics



Microsoft Intune admin center [redacted]

Home > Tenant admin

Tenant admin | Diagnostics settings

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
IntuneLogs	-	-	[redacted]	-	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices
- Windows365AuditLogs

Home > Tenant admin | Diagnostics settings >

Diagnostic setting

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name IntuneLogs

Logs

Categories

- ☑ AuditLogs
- ☑ OperationalLogs
- ☑ DeviceComplianceOrg
- ☑ Devices

Destination details

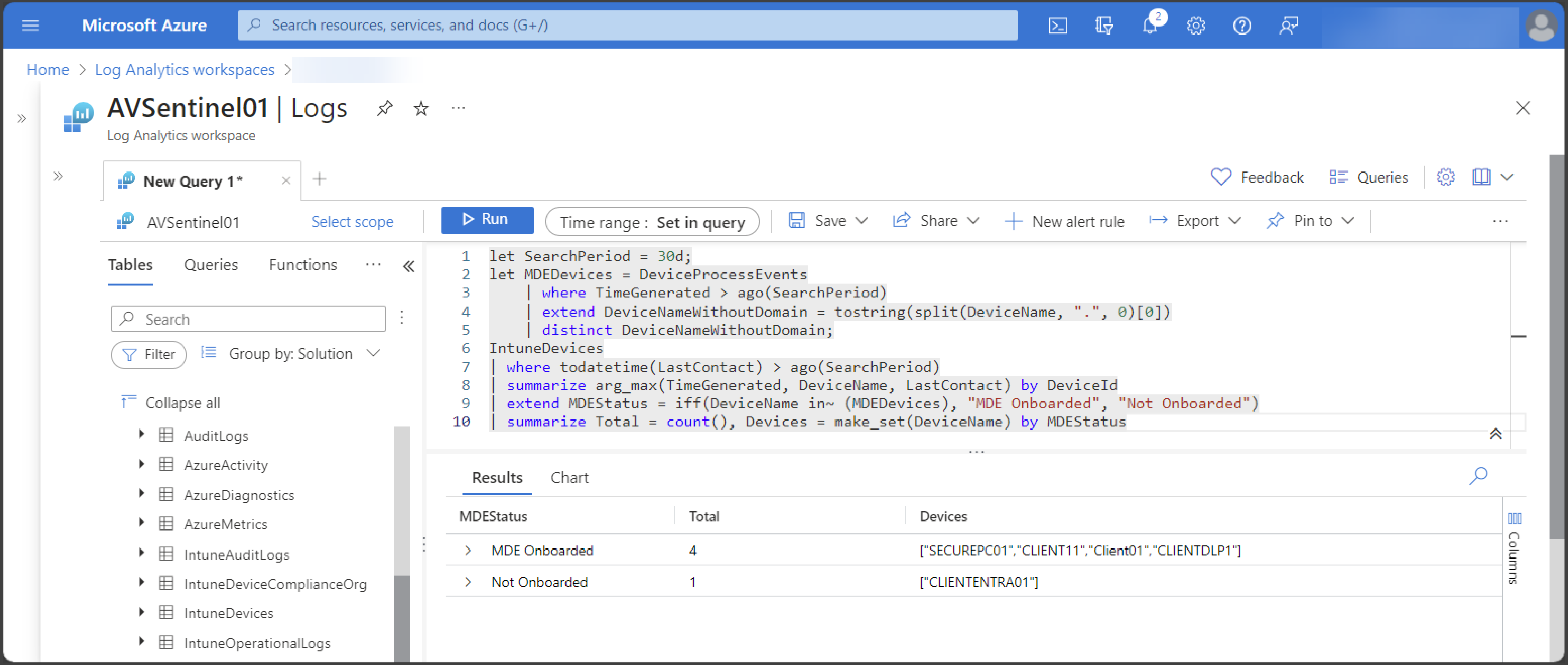
☑ Send to Log Analytics workspace

Subscription: Microsoft Azure Sponsorship

Log Analytics workspace: [redacted]

☐ Archive to a storage account

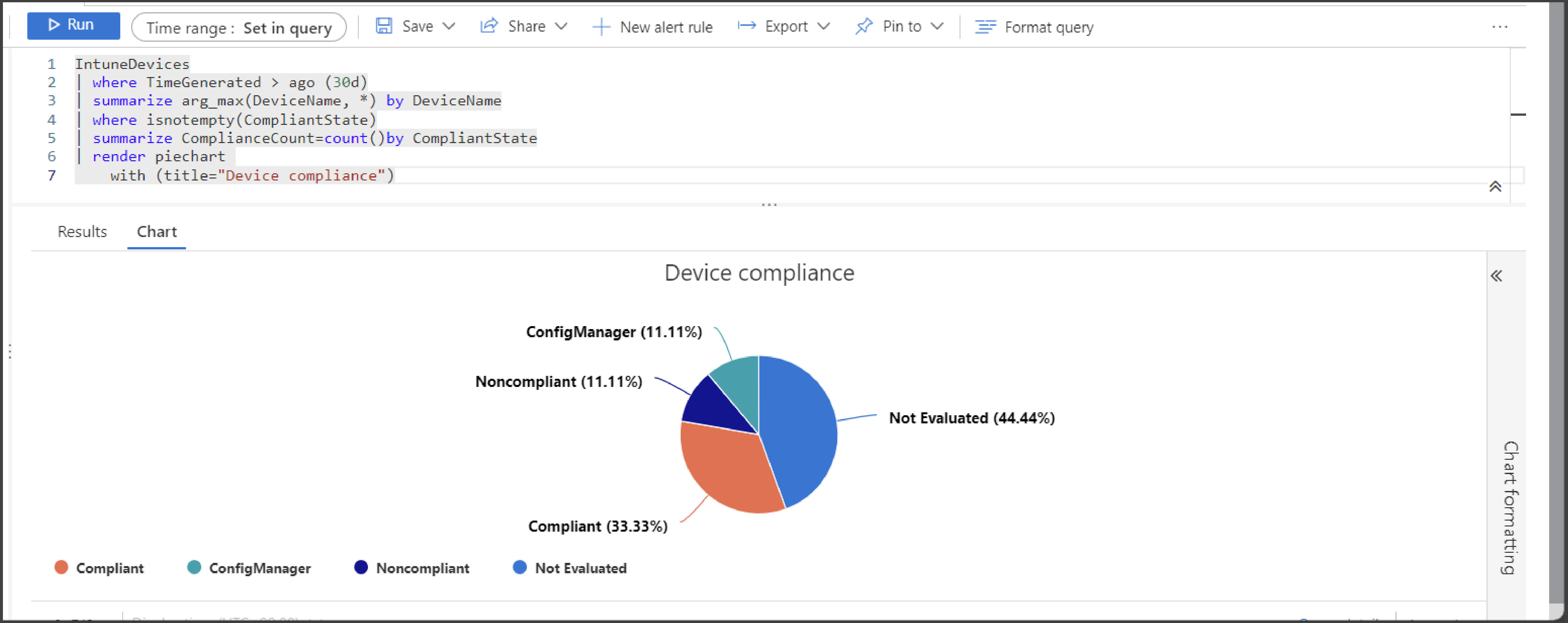
This query compares devices in Intune and Microsoft Defender for Endpoint



```
let SearchPeriod = 30d;
let MDEDevices = DeviceProcessEvents
    | where TimeGenerated > ago(SearchPeriod)
    | extend DeviceNameWithoutDomain = tostring(split(DeviceName, ".", 0)[0])
    | distinct DeviceNameWithoutDomain;
IntuneDevices
| where todatetime(LastContact) > ago(SearchPeriod)
| summarize arg_max(TimeGenerated, DeviceName, LastContact) by DeviceId
| extend MDEStatus = iff(DeviceName in~ (MDEDevices), "MDE Onboarded", "Not Onboarded")
| summarize Total = count(), Devices = make_set(DeviceName) by MDEStatus
```

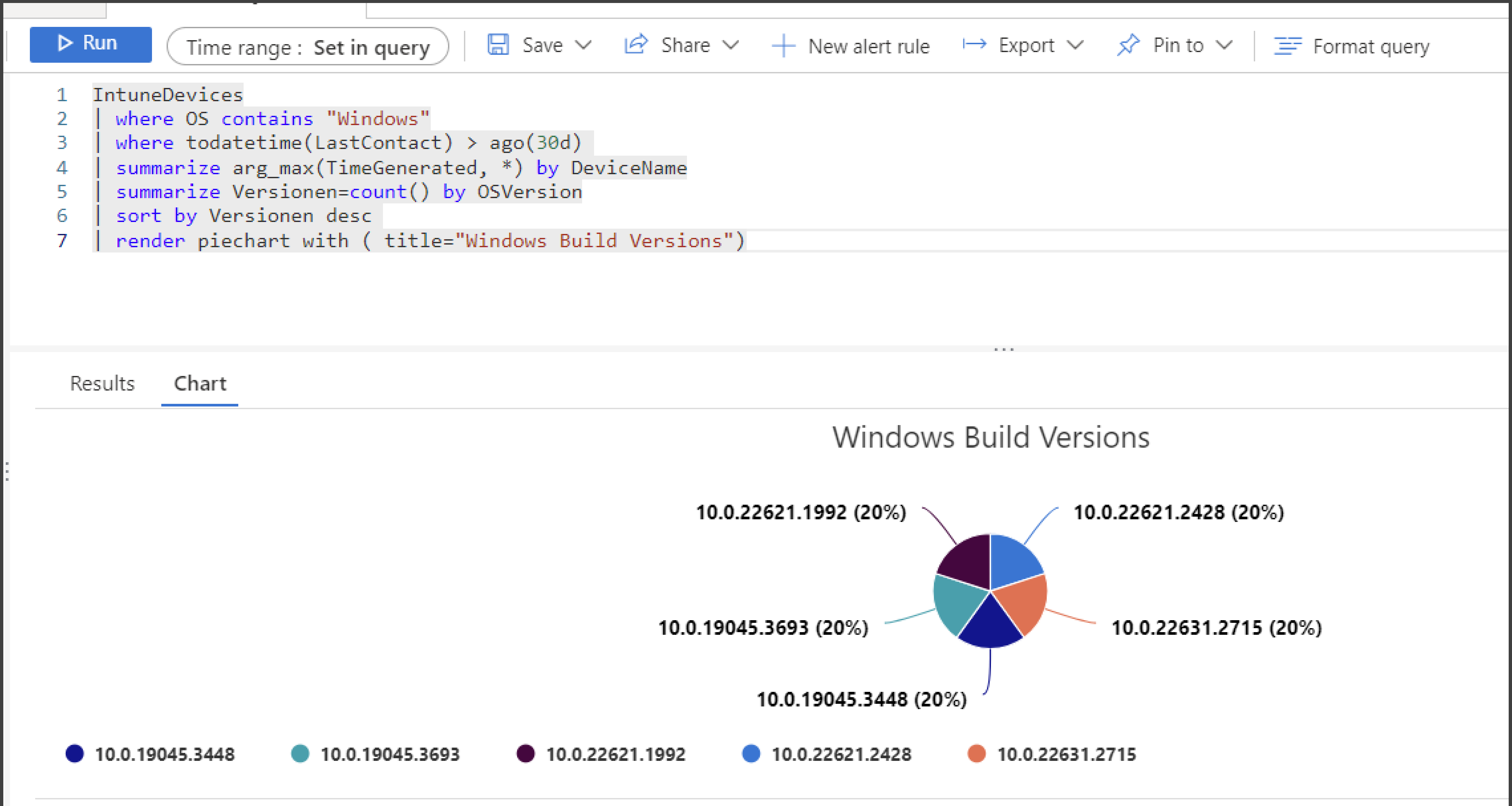
MDEStatus	Total	Devices
MDE Onboarded	4	["SECUREPC01","CLIENT11","Client01","CLIENTDLP1"]
Not Onboarded	1	["CLIENTENTRA01"]

Device - Visualize device compliance



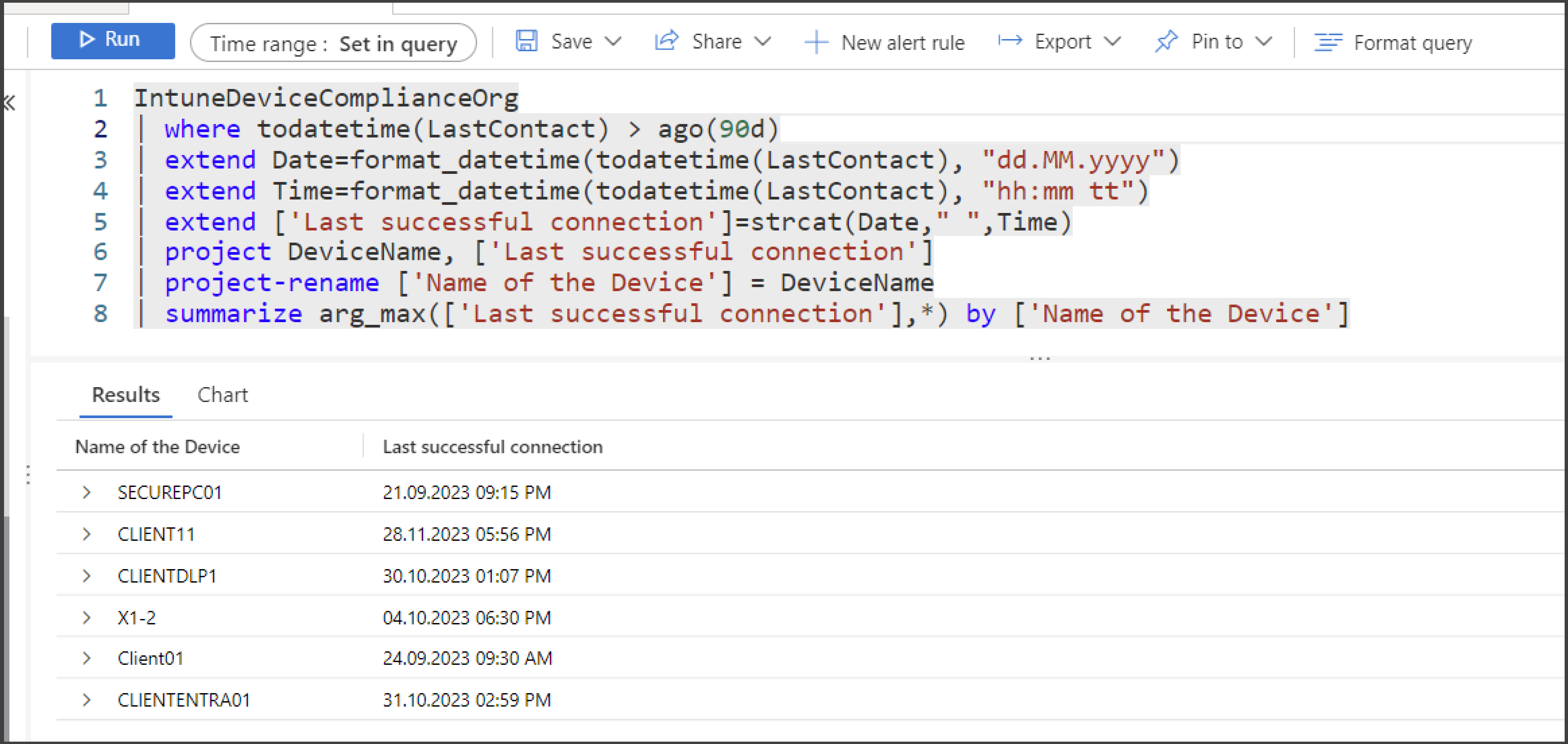
```
IntuneDevices
| where TimeGenerated > ago (30d)
| summarize arg_max(DeviceName, *) by DeviceName
| where isnotempty(CompliantState)
| summarize ComplianceCount=count()by CompliantState
| render piechart
    with (title="Device compliance")
```

Device-VisualizeWindowsVersions



```
IntuneDevices
| where OS contains "Windows"
| where todatetime(LastContact) > ago(30d)
| summarize arg_max(TimeGenerated, *) by DeviceName
| summarize Versionen=count() by OSVersion
| sort by Versionen desc
| render piechart with ( title="Windows Build Versions")
```

Device-LastTimeTheDeviceWasActive

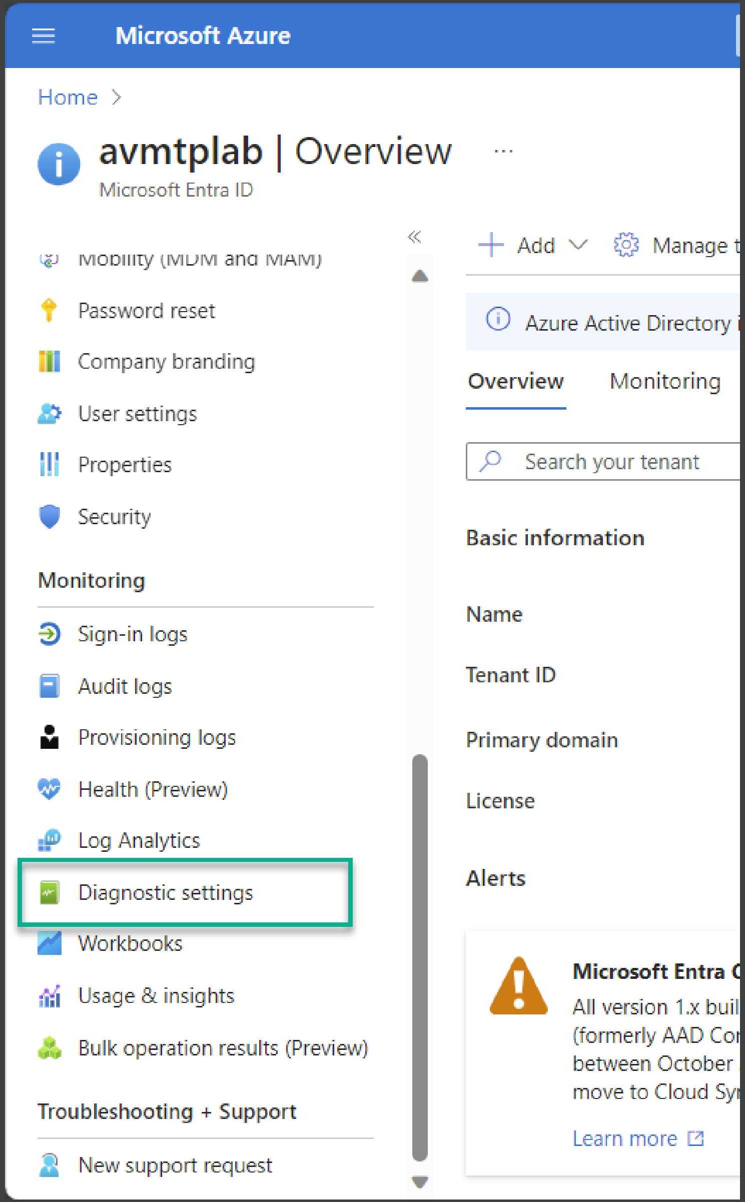


```
IntuneDeviceComplianceOrg
| where todatetime(LastContact) > ago(90d)
| extend Date=format_datetime(todatetime(LastContact), "dd.MM.yyyy")
| extend Time=format_datetime(todatetime(LastContact), "hh:mm tt")
| extend ['Last successful connection']=strcat(Date," ",Time)
| project DeviceName, ['Last successful connection']
| project-rename ['Name of the Device'] = DeviceName
| summarize arg_max(['Last successful connection'],*) by ['Name of the Device']
```

Name of the Device	Last successful connection
SECUREPC01	21.09.2023 09:15 PM
CLIENT11	28.11.2023 05:56 PM
CLIENTDLP1	30.10.2023 01:07 PM
X1-2	04.10.2023 06:30 PM
Client01	24.09.2023 09:30 AM
CLIENTENTRA01	31.10.2023 02:59 PM

geekmania

Bring your Entra ID Sign in Logs into Log Analytics



Microsoft Azure

Home >

avmtplab | Overview ...

Microsoft Entra ID

Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring

- Sign-in logs
- Audit logs
- Provisioning logs
- Health (Preview)
- Log Analytics
- Diagnostic settings
- Workbooks
- Usage & insights
- Bulk operation results (Preview)

Troubleshooting + Support

- New support request

Basic information

Name

Tenant ID

Primary domain

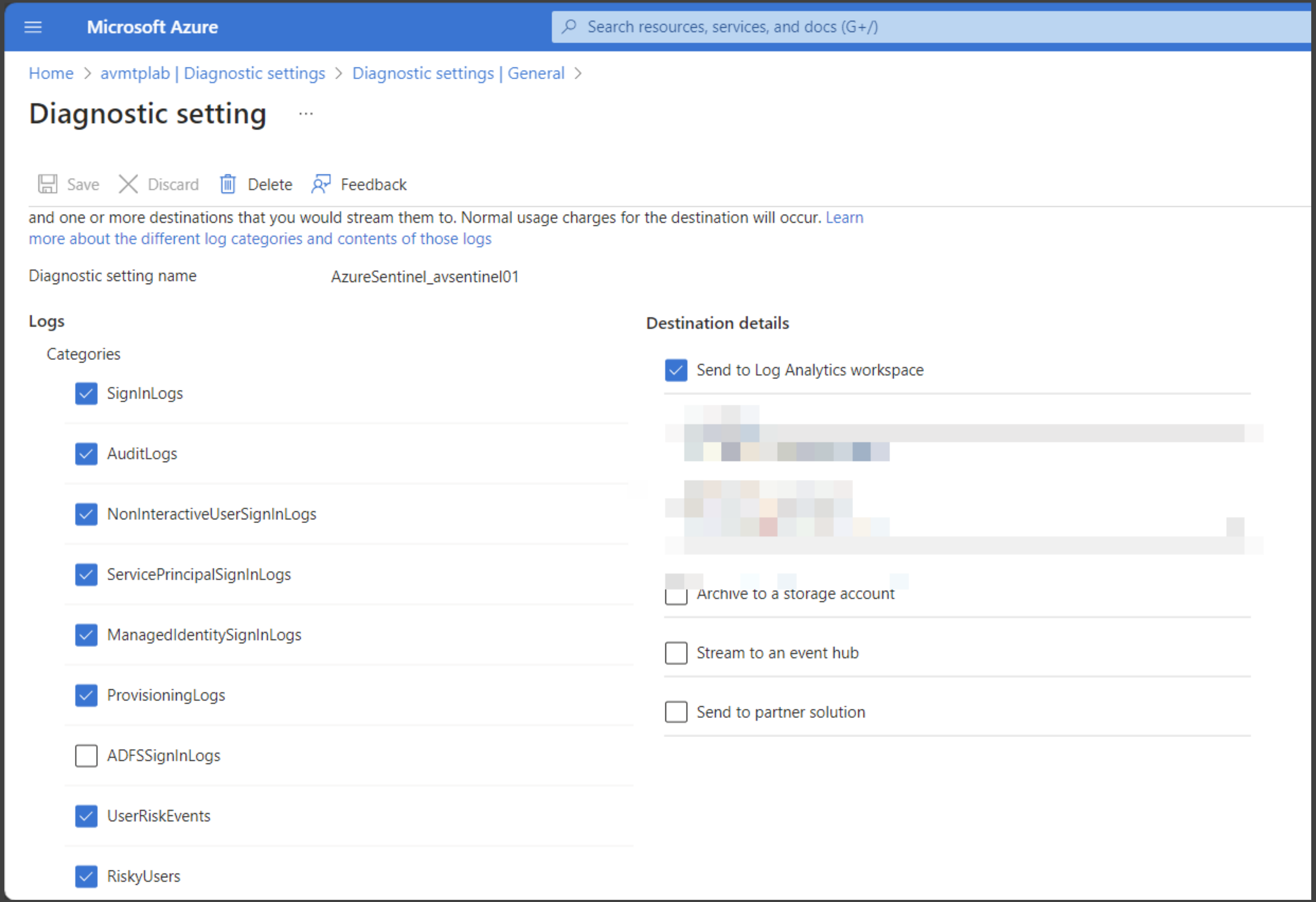
License

Alerts

Microsoft Entra C

All version 1.x buil
(formerly AAD Co
between October
move to Cloud Sy

Learn more



Microsoft Azure

Home > avmtplab | Diagnostic settings > Diagnostic settings | General >

Diagnostic setting ...

and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name AzureSentinel_avsentinel01

Logs

Categories

- ☑ SignInLogs
- ☑ AuditLogs
- ☑ NonInteractiveUserSignInLogs
- ☑ ServicePrincipalSignInLogs
- ☑ ManagedIdentitySignInLogs
- ☑ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☑ UserRiskEvents
- ☑ RiskyUsers

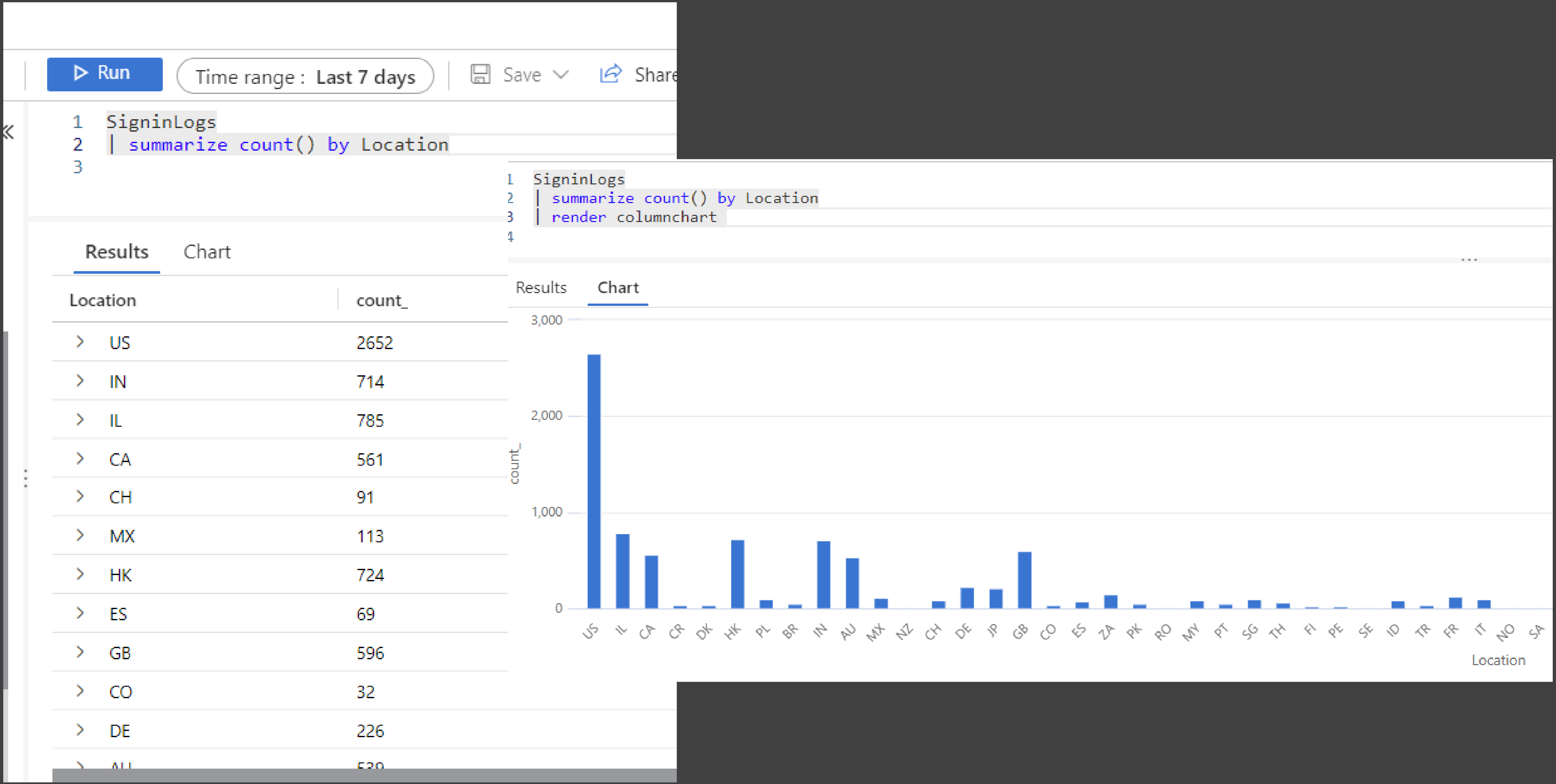
Destination details

- ☑ Send to Log Analytics workspace

[redacted]

- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

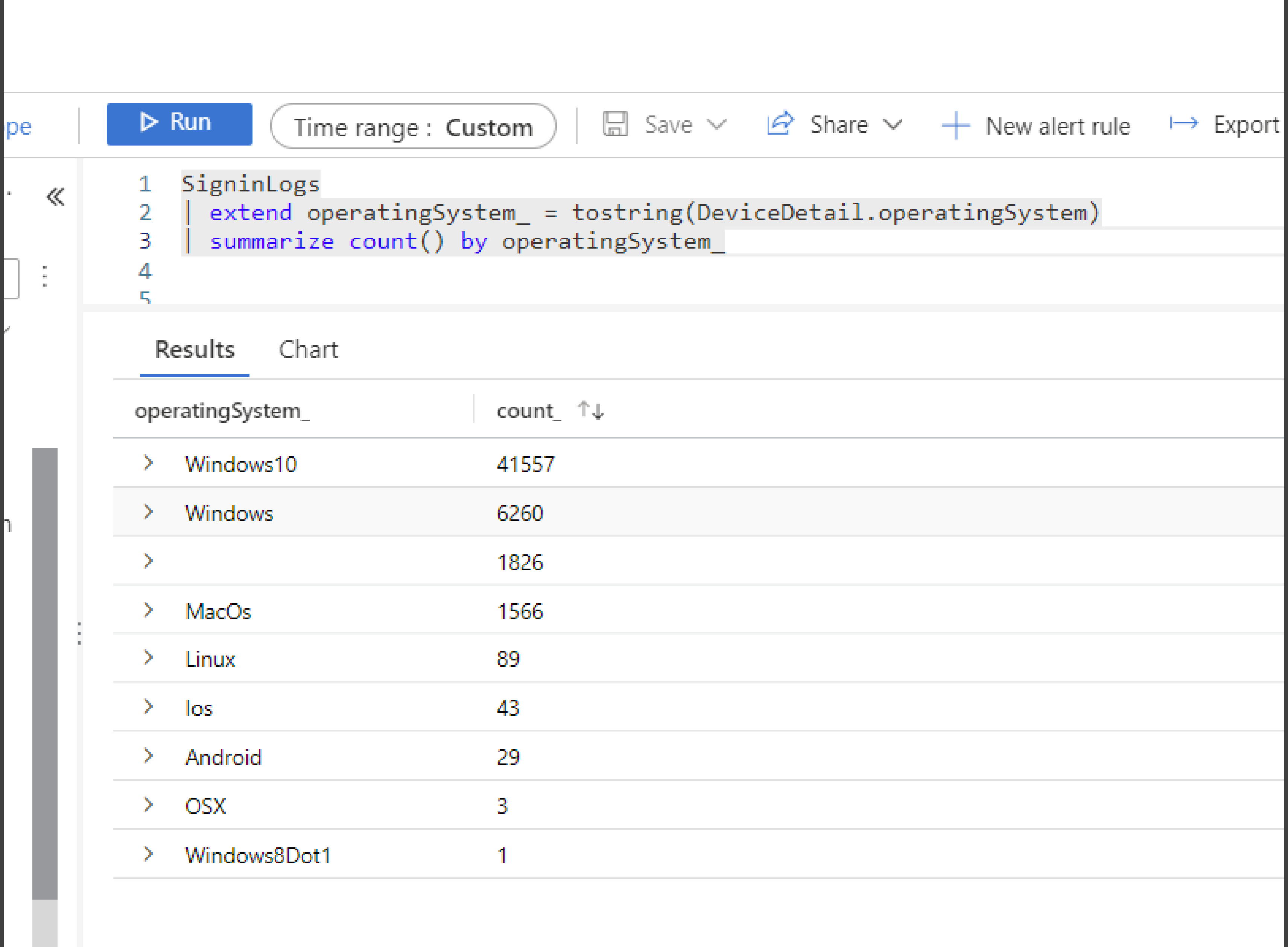
geekmania



```
SigninLogs
| summarize count() by Location
```

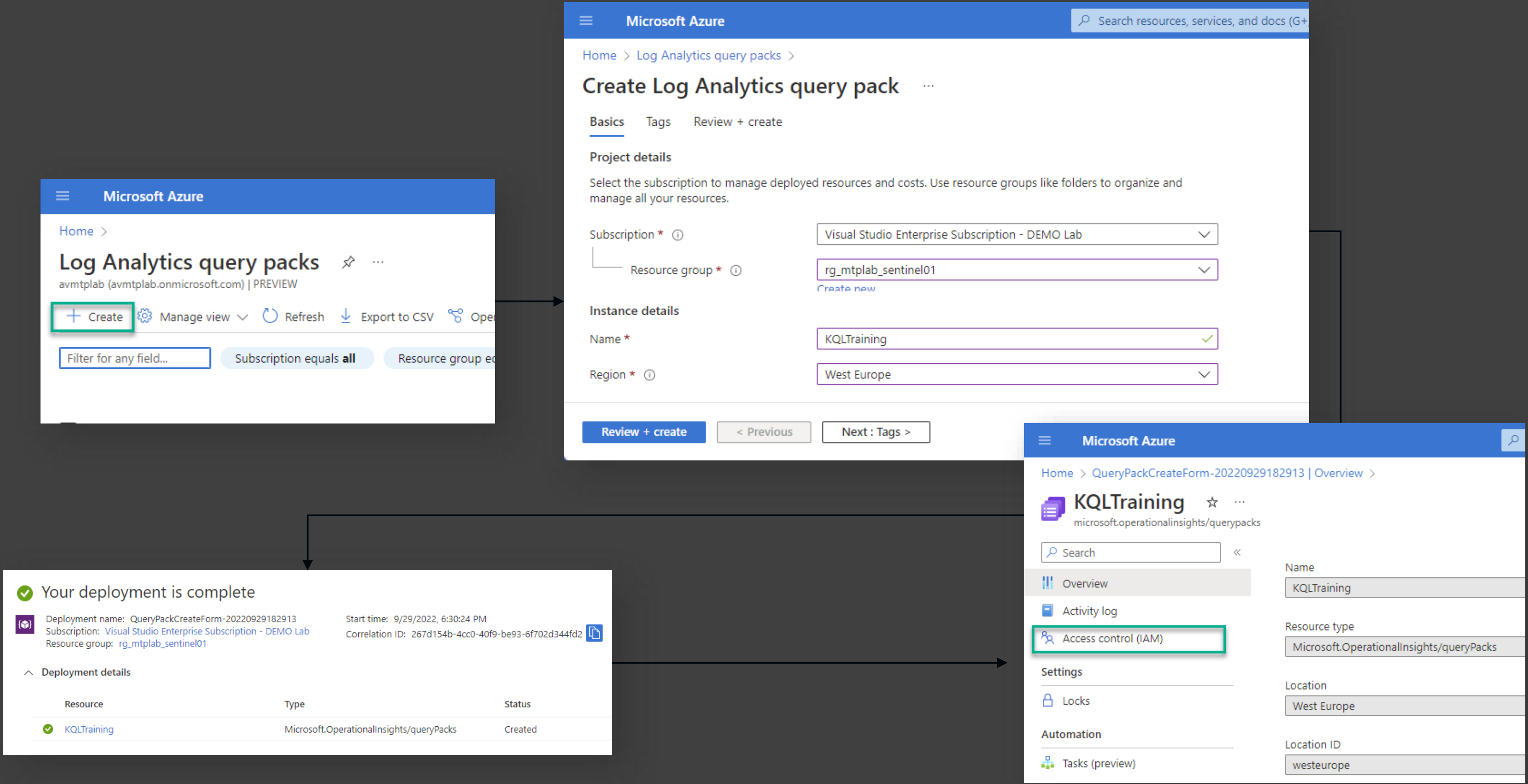
Location	count_
US	2652
IN	714
IL	785
CA	561
CH	91
MX	113
HK	724
ES	69
GB	596
CO	32
DE	226
AU	539

```
SigninLogs
| summarize count() by Location
| render columnchart
```



```
SigninLogs
| extend operatingSystem_ = tostring(DeviceDetail.operatingSystem)
| summarize count() by operatingSystem_
```

operatingSystem_	count_
Windows10	41557
Windows	6260
	1826
MacOs	1566
Linux	89
Ios	43
Android	29
OSX	3
Windows8Dot1	1



Microsoft Azure

Home >

Log Analytics query packs

avmtplab (avmtplab.onmicrosoft.com) | PREVIEW

Microsoft Azure

Home > Log Analytics query packs >

Create Log Analytics query pack

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise Subscription - DEMO Lab

Resource group * : rg_mtplab_sentinel01

Instance details

Name * : KQLTraining

Region * : West Europe

Microsoft Azure

Home > QueryPackCreateForm-20220929182913 | Overview >

KQLTraining

microsoft.operationalinsights/querypacks

Name: KQLTraining

Resource type: Microsoft.OperationalInsights/queryPacks

Location: West Europe

Location ID: westeurope

Your deployment is complete

Deployment name: QueryPackCreateForm-20220929182913

Subscription: Visual Studio Enterprise Subscription - DEMO Lab

Resource group: rg_mtplab_sentinel01

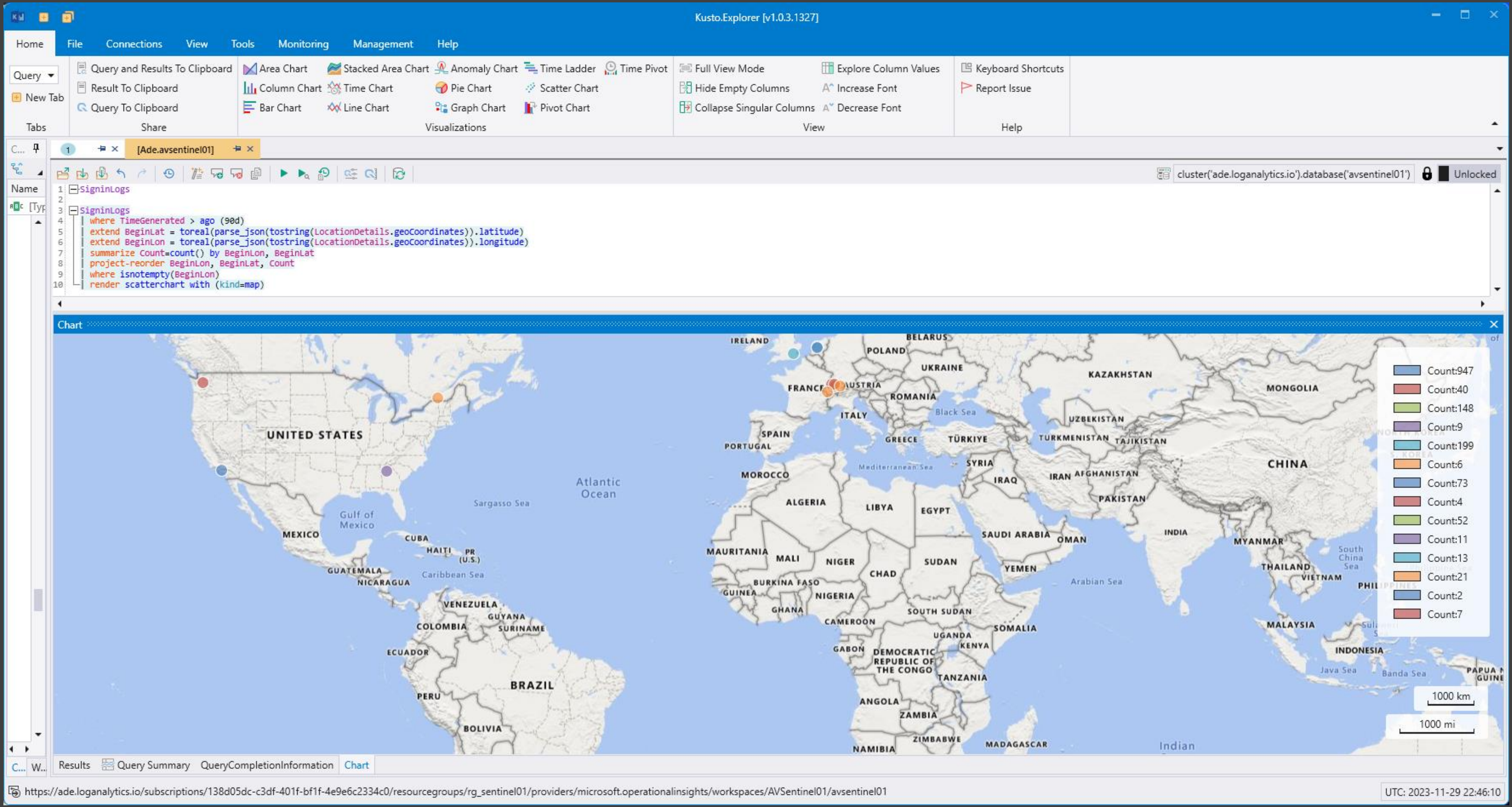
Start time: 9/29/2022, 6:30:24 PM

Correlation ID: 267d154b-4cc0-40f9-be93-6f702d344fd2

Deployment details

Resource	Type	Status
KQLTraining	Microsoft.OperationalInsights/queryPacks	Created

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/tools/kusto-explorer



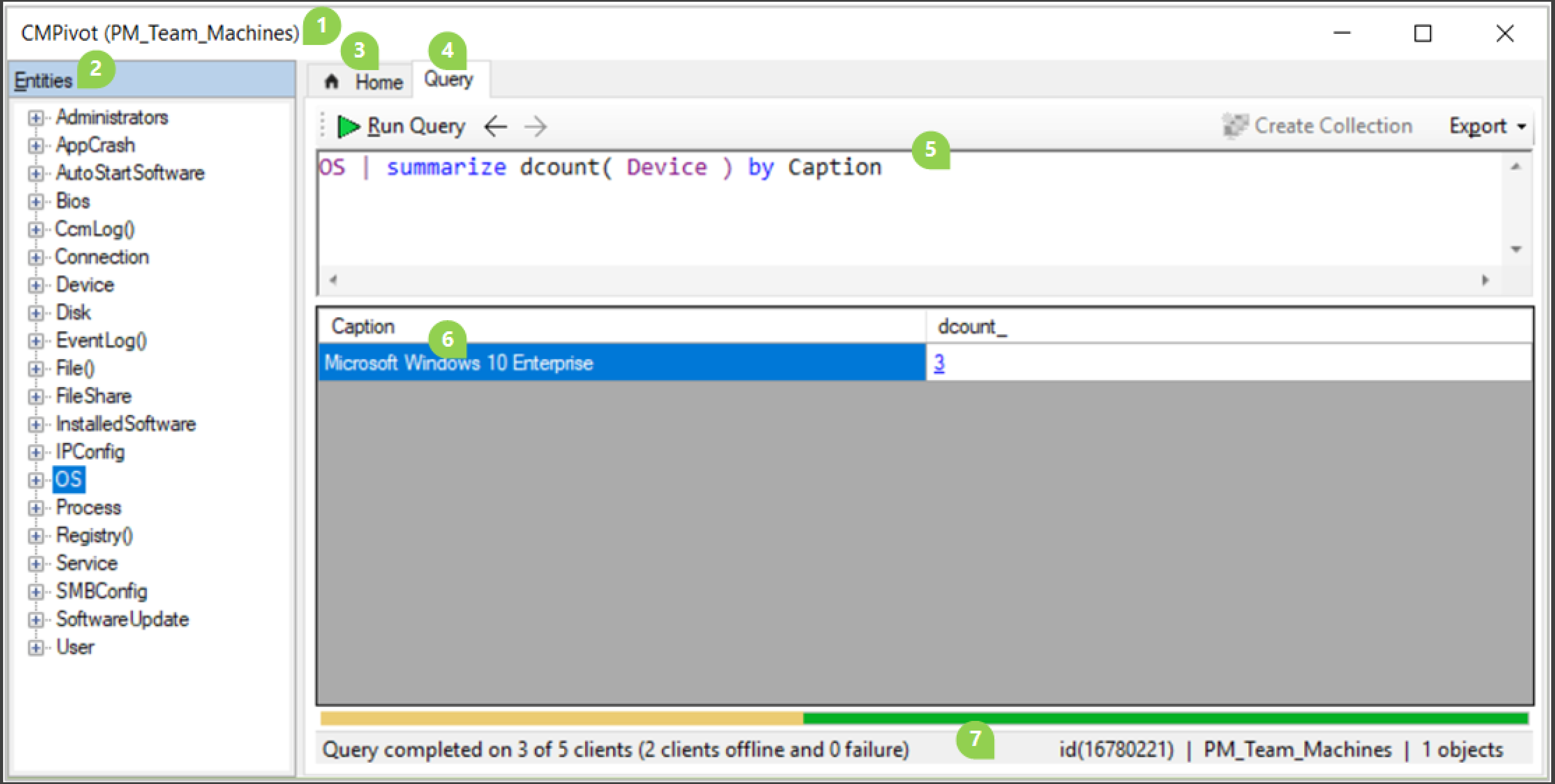
cluster('ade.loganalytics.io').database('avsentinel01')

```
SigninLogs

SigninLogs
| where TimeGenerated > ago (90d)
| extend BeginLat = toreal(parse_json(tostring(LocationDetails.geoCoordinates)).latitude)
| extend BeginLon = toreal(parse_json(tostring(LocationDetails.geoCoordinates)).longitude)
| summarize Count=count() by BeginLon, BeginLat
| project-reorder BeginLon, BeginLat, Count
| where isnotempty(BeginLon)
| render scatterchart with (kind=map)
```

https://ade.loganalytics.io/subscriptions/138d05dc-c3df-401f-bf1f-4e9e6c2334c0/resourcegroups/rg_sentinel01/providers/microsoft.operationalinsights/workspaces/AVSentinel01/avsentinel01

UTC: 2023-11-29 22:46:10

CMPivot in ConfigMgr



```
OS | summarize dcount( Device ) by Caption
```

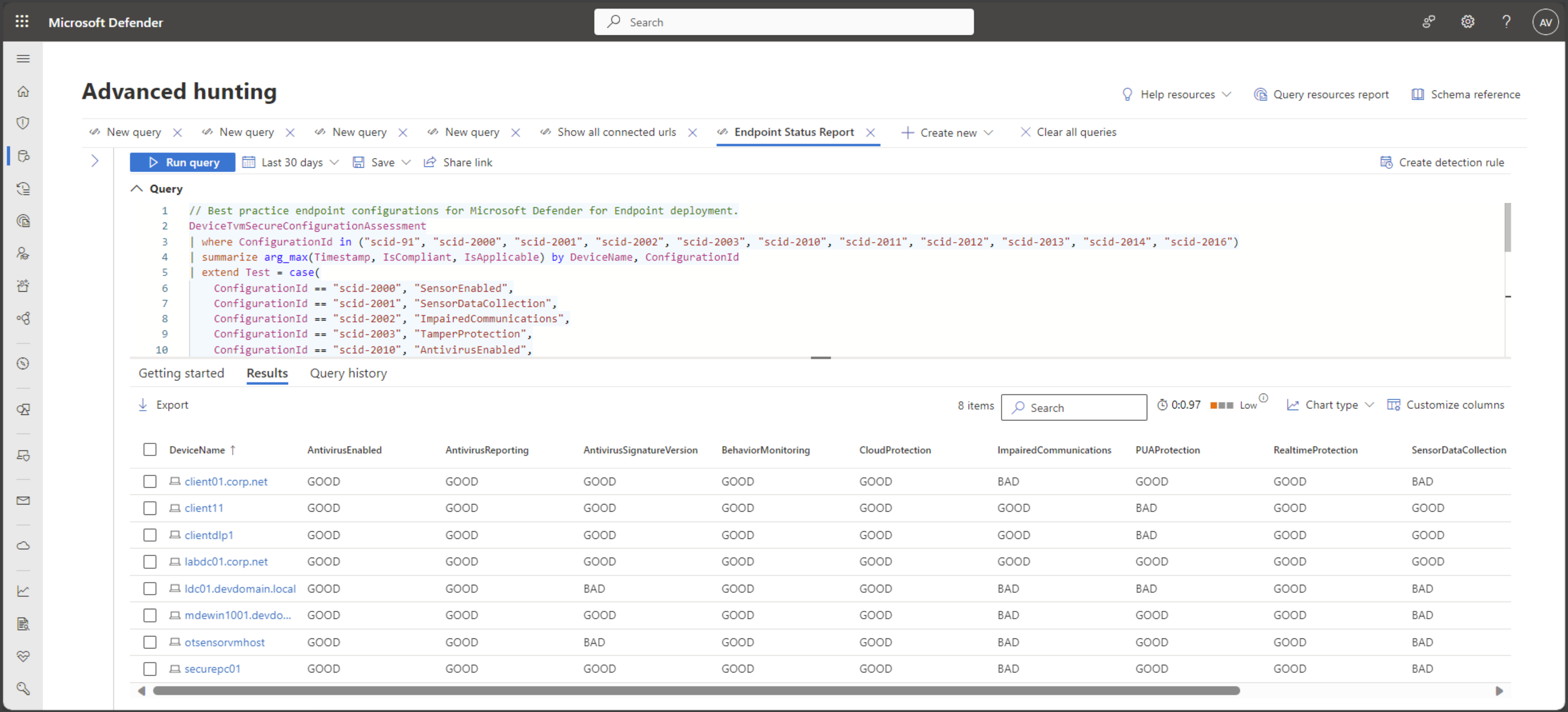
Caption	dcount_
Microsoft Windows 10 Enterprise	3

```
Query completed on 3 of 5 clients (2 clients offline and 0 failure)        id(16780221) | PM_Team_Machines | 1 objects
```

https://learn.microsoft.com/en-us/mem/configmgr/core/servers/manage/cmpivot

geekmania

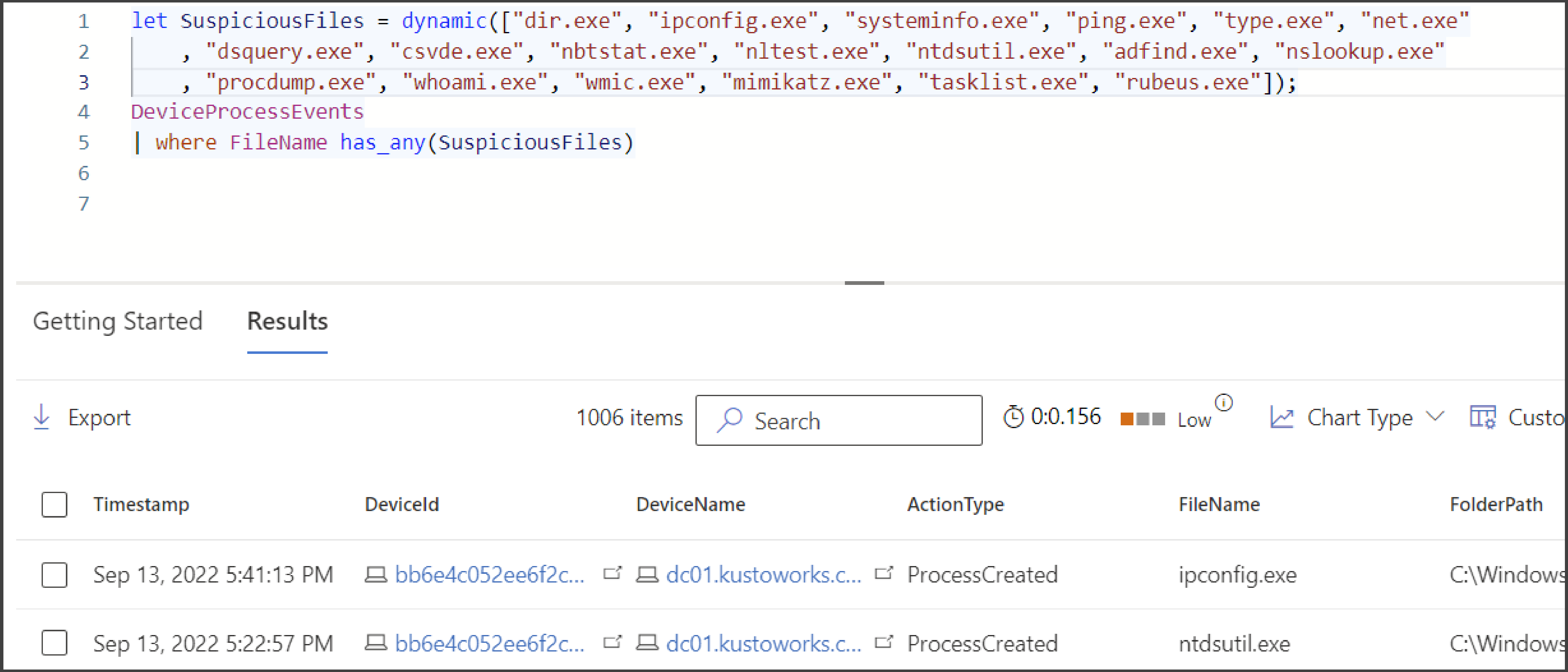
Advanced Hunting in Defender XDR



```
// Best practice endpoint configurations for Microsoft Defender for Endpoint deployment.
DeviceTvmSecureConfigurationAssessment
| where ConfigurationId in ("scid-91", "scid-2000", "scid-2001", "scid-2002", "scid-2003", "scid-2010", "scid-2011", "scid-2012", "scid-2013", "scid-2014", "scid-2016")
| summarize arg_max(Timestamp, IsCompliant, IsApplicable) by DeviceName, ConfigurationId
| extend Test = case(
    ConfigurationId == "scid-2000", "SensorEnabled",
    ConfigurationId == "scid-2001", "SensorDataCollection",
    ConfigurationId == "scid-2002", "ImpairedCommunications",
    ConfigurationId == "scid-2003", "TamperProtection",
    ConfigurationId == "scid-2010", "AntivirusEnabled",
```

DeviceName ↑	AntivirusEnabled	AntivirusReporting	AntivirusSignatureVersion	BehaviorMonitoring	CloudProtection	ImpairedCommunications	PUAProtection	RealtimeProtection	SensorDataCollection
client01.corp.net	GOOD	GOOD	GOOD	GOOD	GOOD	BAD	GOOD	GOOD	BAD
client11	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	BAD	GOOD	GOOD
clientdlp1	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	BAD	GOOD	GOOD
labdc01.corp.net	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
ldc01.devdomain.local	GOOD	GOOD	BAD	GOOD	GOOD	BAD	BAD	GOOD	BAD
mdewin1001.devdo...	GOOD	GOOD	GOOD	GOOD	GOOD	BAD	GOOD	GOOD	BAD
otsensorvmhost	GOOD	GOOD	BAD	GOOD	GOOD	BAD	GOOD	GOOD	BAD
securepc01	GOOD	GOOD	GOOD	GOOD	GOOD	BAD	GOOD	GOOD	BAD

Advanced Hunting in Defender XDR



```
let SuspiciousFiles = dynamic(["dir.exe", "ipconfig.exe", "systeminfo.exe", "ping.exe", "type.exe", "net.exe"
    , "dsquery.exe", "csvde.exe", "nbtstat.exe", "nltest.exe", "ntdsutil.exe", "adfind.exe", "nslookup.exe"
    , "procdump.exe", "whoami.exe", "wmic.exe", "mimikatz.exe", "tasklist.exe", "rubeus.exe"]);
DeviceProcessEvents
| where FileName has_any(SuspiciousFiles)
```

1006 items

0:0.156

□	Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
□	Sep 13, 2022 5:41:13 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	ipconfig.exe	C:\Windows
□	Sep 13, 2022 5:22:57 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	ntdsutil.exe	C:\Windows

geekmania

KQL Operators

geekmania

KQL – Most used operators

KQL – String Operators

Operator	Description	Case-Sensitive	Example (yields `true`)
==	Equals	Yes	`"aBc" == "aBc"`
!=	Not equals	Yes	`"abc" != "ABC"`
=~	Equals	No	`"abc" =~ "ABC"`
!~	Not equals	No	`"aBc" !~ "xyz"`
contains	RHS occurs as a subsequence of LHS	No	`"FabriKam" contains "BRik"`
!contains	RHS doesn't occur in LHS	No	`"Fabrikam" !contains "xyz"`
contains_cs	RHS occurs as a subsequence of LHS	Yes	`"FabriKam" contains_cs "Kam"`
!contains_cs	RHS doesn't occur in LHS	Yes	`"Fabrikam" !contains_cs "Kam"`
endswith	RHS is a closing subsequence of LHS	No	`"Fabrikam" endswith "Kam"`
!endswith	RHS isn't a closing subsequence of LHS	No	`"Fabrikam" !endswith "brik"`
endswith_cs	RHS is a closing subsequence of LHS	Yes	`"Fabrikam" endswith_cs "kam"`
!endswith_cs	RHS isn't a closing subsequence of LHS	Yes	`"Fabrikam" !endswith_cs "brik"`
has	Right-hand-side (RHS) is a whole term in left-hand-side (LHS)	No	`"North America" has "america"`
!has	RHS isn't a full term in LHS	No	`"North America" !has "amer"`
has_all	Same as `has` but works on all of the elements	No	`"North and South America" has_all("south", "north")`
has_any	Same as `has` but works on any of the elements	No	`"North America" has_any("south", "north")`
has_cs	RHS is a whole term in LHS	Yes	`"North America" has_cs "America"`
!has_cs	RHS isn't a full term in LHS	Yes	`"North America" !has_cs "amer"`

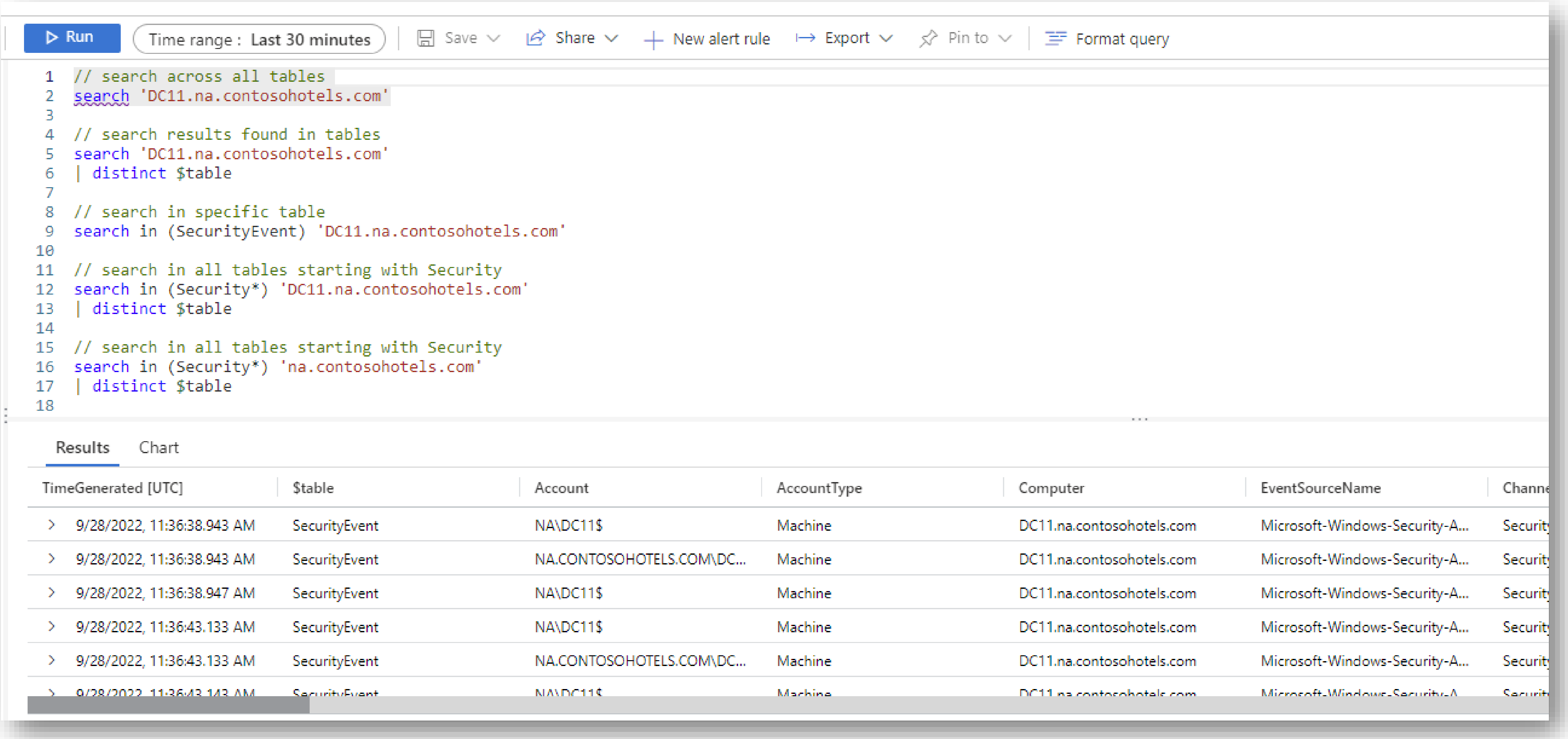
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/datatypes-string-operators

KQL – String Operators

Operator	Description	Case-Sensitive	Example (yields `true`)
hasprefix	RHS is a term prefix in LHS	No	`"North America" hasprefix "ame"`
!hasprefix	RHS isn't a term prefix in LHS	No	`"North America" !hasprefix "mer"`
hasprefix_cs	RHS is a term prefix in LHS	Yes	`"North America" hasprefix_cs "Ame"`
!hasprefix_cs	RHS isn't a term prefix in LHS	Yes	`"North America" !hasprefix_cs "CA"`
hassuffix	RHS is a term suffix in LHS	No	`"North America" hassuffix "ica"`
!hassuffix	RHS isn't a term suffix in LHS	No	`"North America" !hassuffix "americ"`
hassuffix_cs	RHS is a term suffix in LHS	Yes	`"North America" hassuffix_cs "ica"`
!hassuffix_cs	RHS isn't a term suffix in LHS	Yes	`"North America" !hassuffix_cs "icA"`
in	Equals to any of the elements	Yes	`"abc" in ("123", "345", "abc")`
!in	Not equals to any of the elements	Yes	`"bca" !in ("123", "345", "abc")`
in~	Equals to any of the elements	No	`"Abc" in~ ("123", "345", "abc")`
!in~	Not equals to any of the elements	No	`"bCa" !in~ ("123", "345", "ABC")`
matches regex	LHS contains a match for RHS	Yes	`"Fabrikam" matches regex "b.*k"`
startswith	RHS is an initial subsequence of LHS	No	`"Fabrikam" startswith "fab"`
!startswith	RHS isn't an initial subsequence of LHS	No	`"Fabrikam" !startswith "kam"`
startswith_cs	RHS is an initial subsequence of LHS	Yes	`"Fabrikam" startswith_cs "Fab"`
!startswith_cs	RHS isn't an initial subsequence of LHS	Yes	`"Fabrikam" !startswith_cs "fab"`

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/datatypes-string-operators

KQL - search

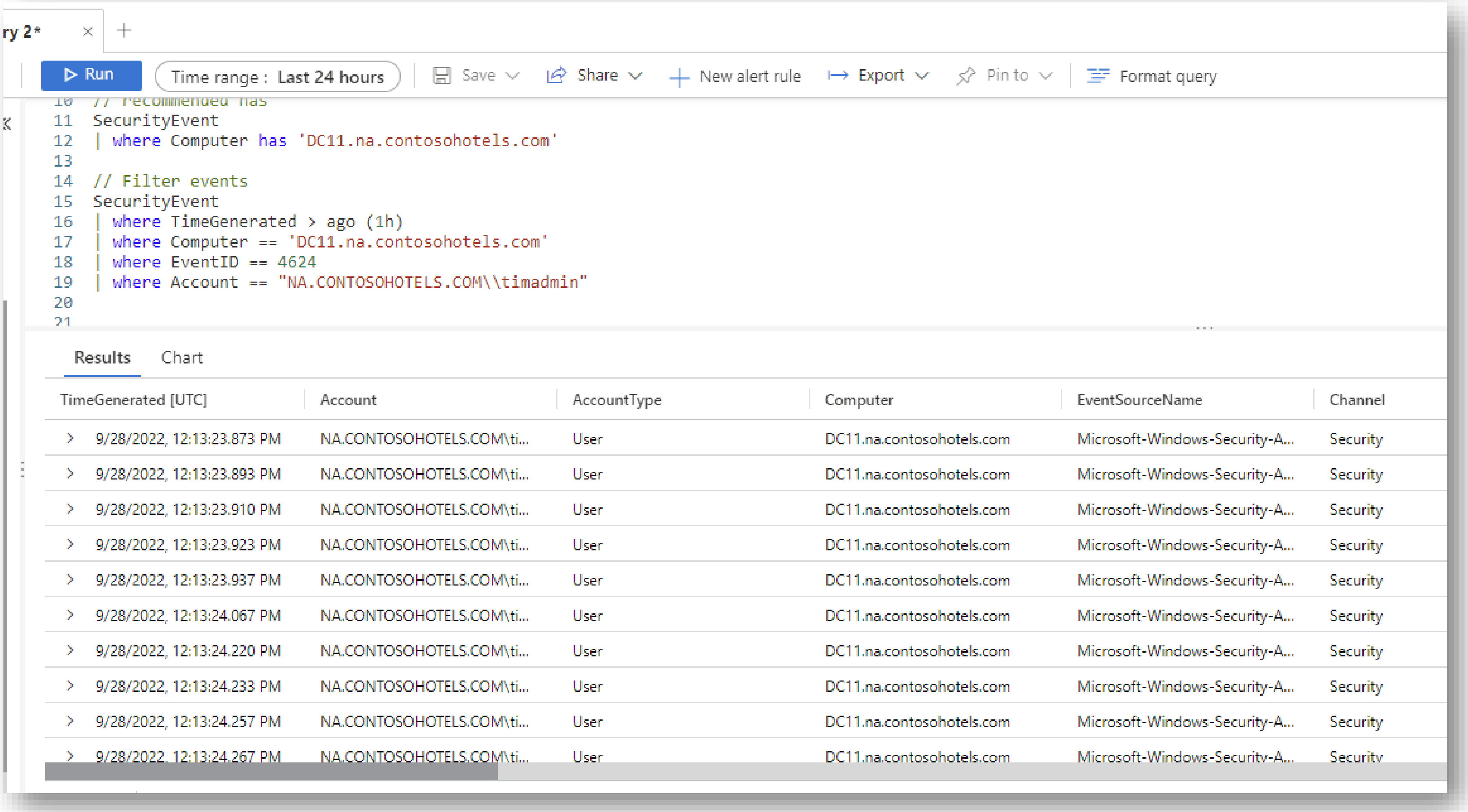


```
// search across all tables
search 'DC11.na.contosohotels.com'

// search results found in tables
search 'DC11.na.contosohotels.com'
| distinct $table

// search in specific table
search in (SecurityEvent) 'DC11.na.contosohotels.com'

// search in all tables starting with Security
search in (Security*) 'DC11.na.contosohotels.com'
| distinct $table

// search in all tables starting with Security
search in (Security*) 'na.contosohotels.com'
| distinct $table

```

TimeGenerated [UTC]	$table	Account	AccountType	Computer	EventSourceName	Channe
9/28/2022, 11:36:38.943 AM	SecurityEvent	NA\DC11$	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 11:36:38.943 AM	SecurityEvent	NA.CONTOSOHOTELS.COM\DC...	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 11:36:38.947 AM	SecurityEvent	NA\DC11$	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 11:36:43.133 AM	SecurityEvent	NA\DC11$	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 11:36:43.133 AM	SecurityEvent	NA.CONTOSOHOTELS.COM\DC...	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 11:36:43.143 AM	SecurityEvent	NA\DC11$	Machine	DC11.na.contosohotels.com	Microsoft-Windows-Security-A	Security

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/searchoperator?pivots=azuremonitor

KQL - where



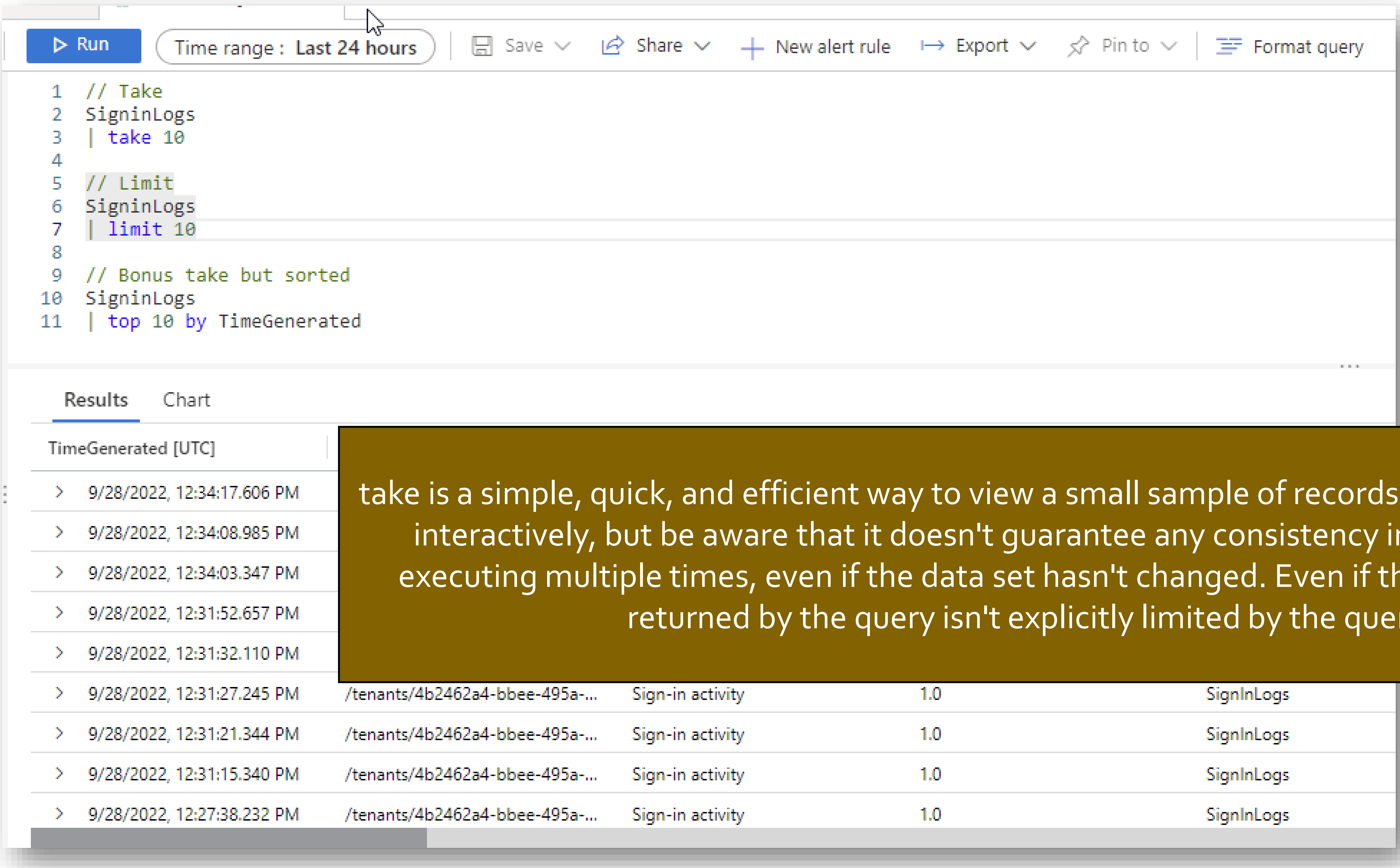
Time range : Last 24 hours

```
// recommended has
SecurityEvent
| where Computer has 'DC11.na.contosohotels.com'

// Filter events
SecurityEvent
| where TimeGenerated > ago (1h)
| where Computer == 'DC11.na.contosohotels.com'
| where EventID == 4624
| where Account == "NA.CONTOSOHOTELS.COM\\timadmin"

```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel
9/28/2022, 12:13:23.873 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:23.893 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:23.910 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:23.923 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:23.937 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:24.067 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:24.220 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:24.233 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:24.257 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security
9/28/2022, 12:13:24.267 PM	NA.CONTOSOHOTELS.COM\ti...	User	DC11.na.contosohotels.com	Microsoft-Windows-Security-A...	Security

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/whereoperator

KQL – take (limit) - top



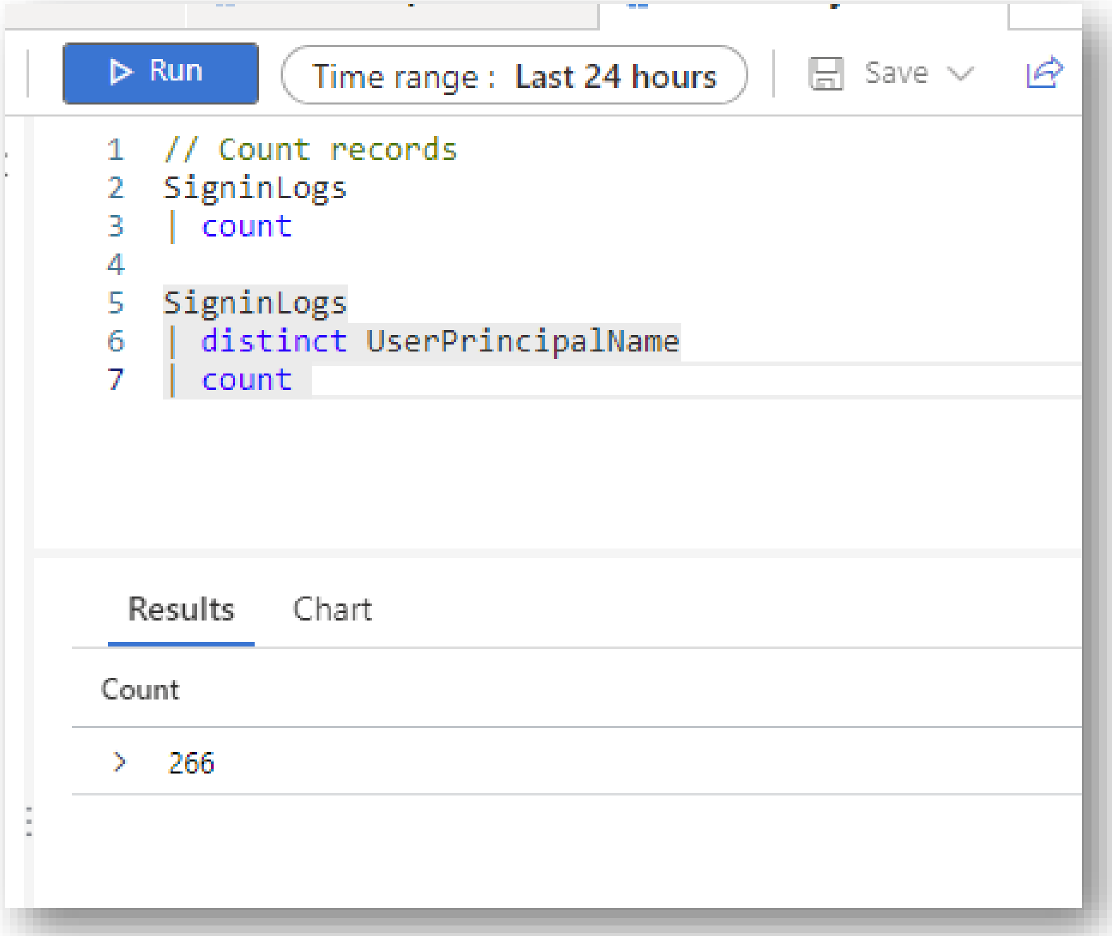
```
// Take
SigninLogs
| take 10

// Limit
SigninLogs
| limit 10

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

TimeGenerated [UTC]				
9/28/2022, 12:34:17.606 PM				
9/28/2022, 12:34:08.985 PM				
9/28/2022, 12:34:03.347 PM				
9/28/2022, 12:31:52.657 PM				
9/28/2022, 12:31:32.110 PM				
9/28/2022, 12:31:27.245 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs
9/28/2022, 12:31:21.344 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs
9/28/2022, 12:31:15.340 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs
9/28/2022, 12:27:38.232 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs

take is a simple, quick, and efficient way to view a small sample of records when browsing data interactively, but be aware that it doesn't guarantee any consistency in its results when executing multiple times, even if the data set hasn't changed. Even if the number of rows returned by the query isn't explicitly limited by the query

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/takeoperator

KQL - count



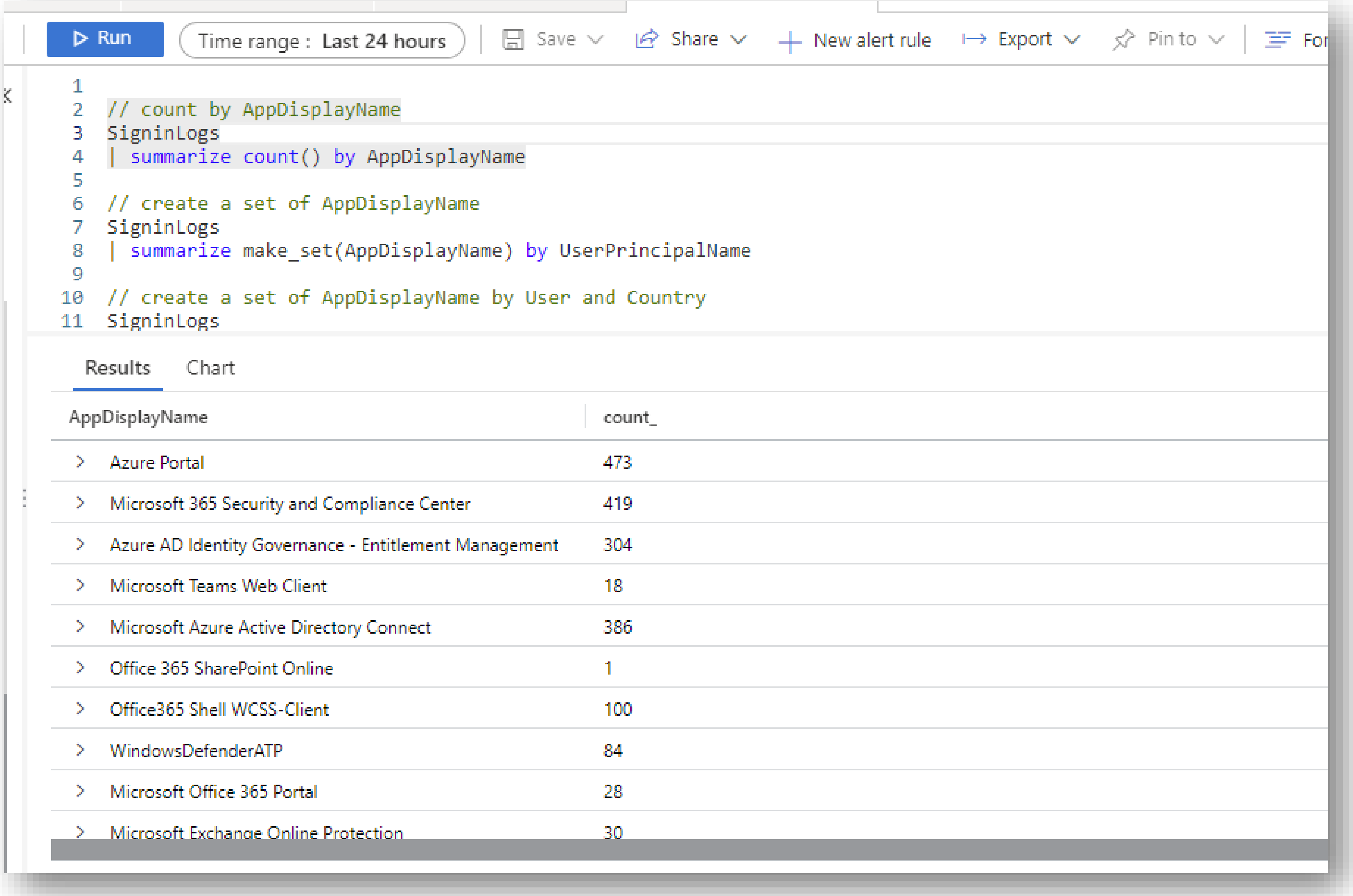
```
// Count records
SigninLogs
| count

SigninLogs
| distinct UserPrincipalName
| count
```

```
Count
> 266
```

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/countoperator

KQL - summarize

Produces a table that aggregates the content of the input table.



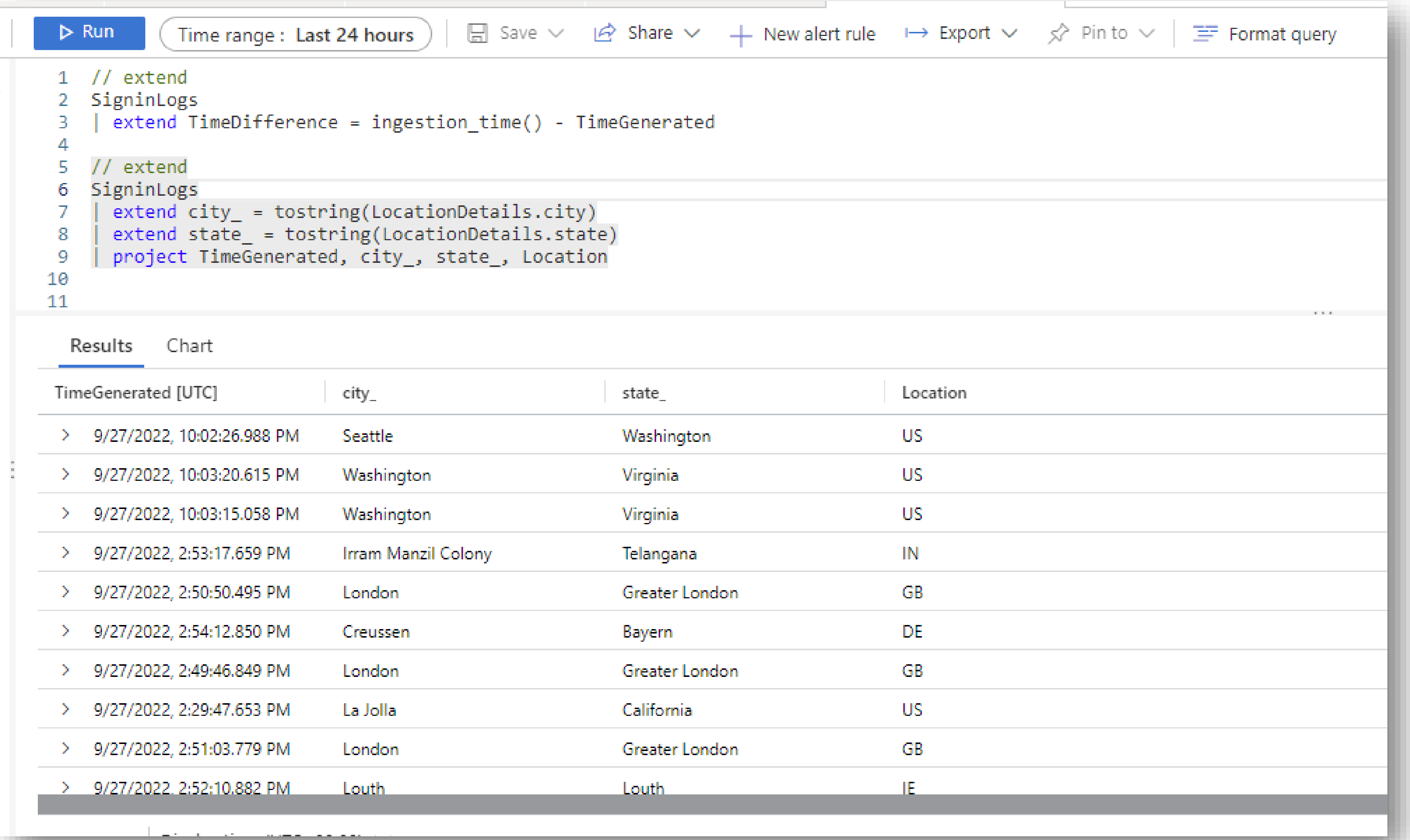
```

// 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
```

AppDisplayName	count_
Azure Portal	473
Microsoft 365 Security and Compliance Center	419
Azure AD Identity Governance - Entitlement Management	304
Microsoft Teams Web Client	18
Microsoft Azure Active Directory Connect	386
Office 365 SharePoint Online	1
Office365 Shell WCSS-Client	100
WindowsDefenderATP	84
Microsoft Office 365 Portal	28
Microsoft Exchange Online Protection	30

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/summarizeoperator

KQL - extend

Create calculated columns and append them to the result set.



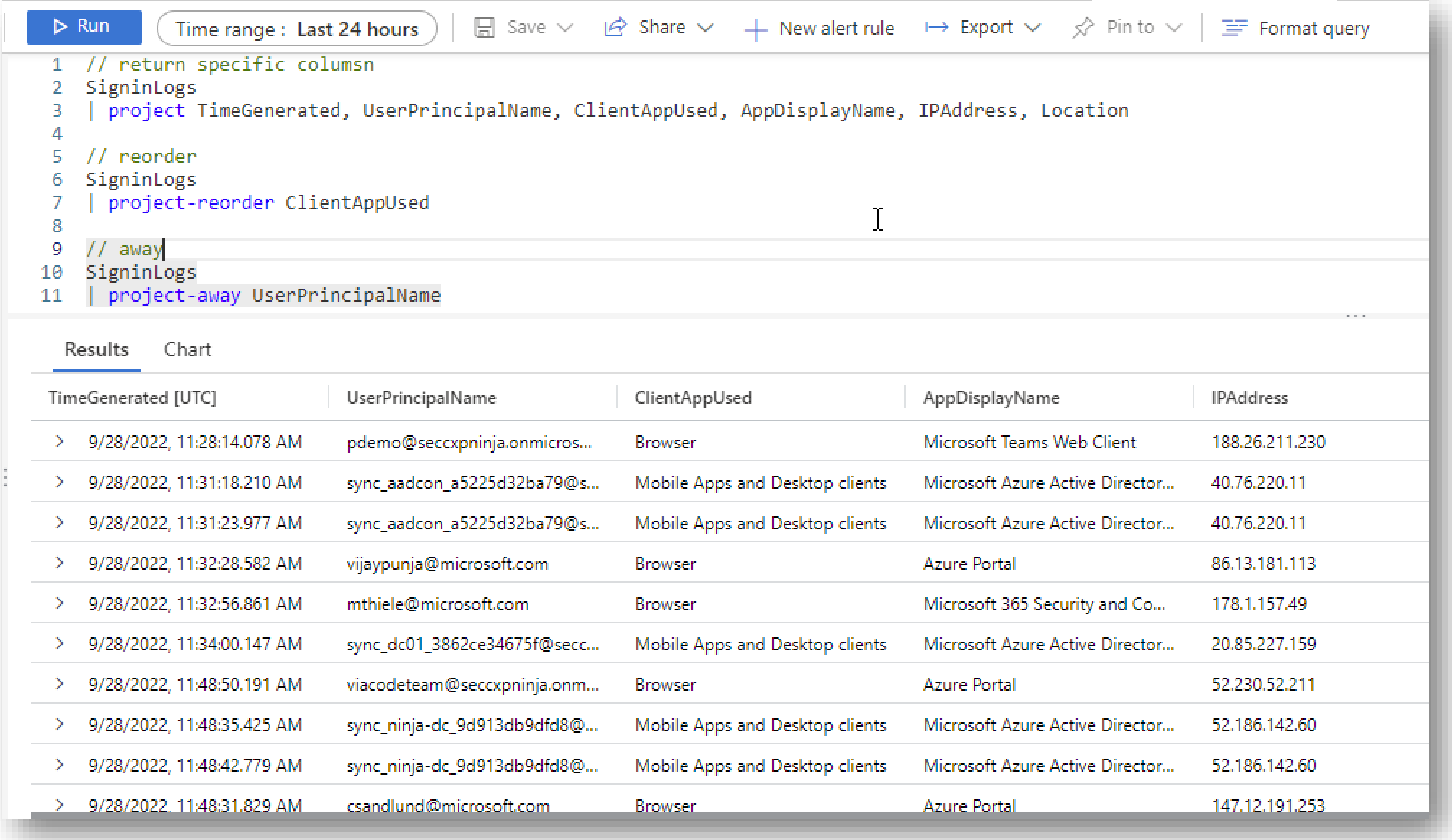
```
// extend
SigninLogs
| extend TimeDifference = ingestion_time() - TimeGenerated

// extend
SigninLogs
| extend city_ = tostring(LocationDetails.city)
| extend state_ = tostring(LocationDetails.state)
| project TimeGenerated, city_, state_, Location
```

TimeGenerated [UTC]	city_	state_	Location
9/27/2022, 10:02:26.988 PM	Seattle	Washington	US
9/27/2022, 10:03:20.615 PM	Washington	Virginia	US
9/27/2022, 10:03:15.058 PM	Washington	Virginia	US
9/27/2022, 2:53:17.659 PM	Irram Manzil Colony	Telangana	IN
9/27/2022, 2:50:50.495 PM	London	Greater London	GB
9/27/2022, 2:54:12.850 PM	Creussen	Bayern	DE
9/27/2022, 2:49:46.849 PM	London	Greater London	GB
9/27/2022, 2:29:47.653 PM	La Jolla	California	US
9/27/2022, 2:51:03.779 PM	London	Greater London	GB
9/27/2022, 2:52:10.882 PM	Louth	Louth	IE

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/extendoperator

KQL - project

Select the columns to include, rename or drop, and insert new computed columns.



```
// return specific columsn
SigninLogs
| project TimeGenerated, UserPrincipalName, ClientAppUsed, AppDisplayName, IPAddress, Location

// reorder
SigninLogs
| project-reorder ClientAppUsed

// away
SigninLogs
| project-away UserPrincipalName
```

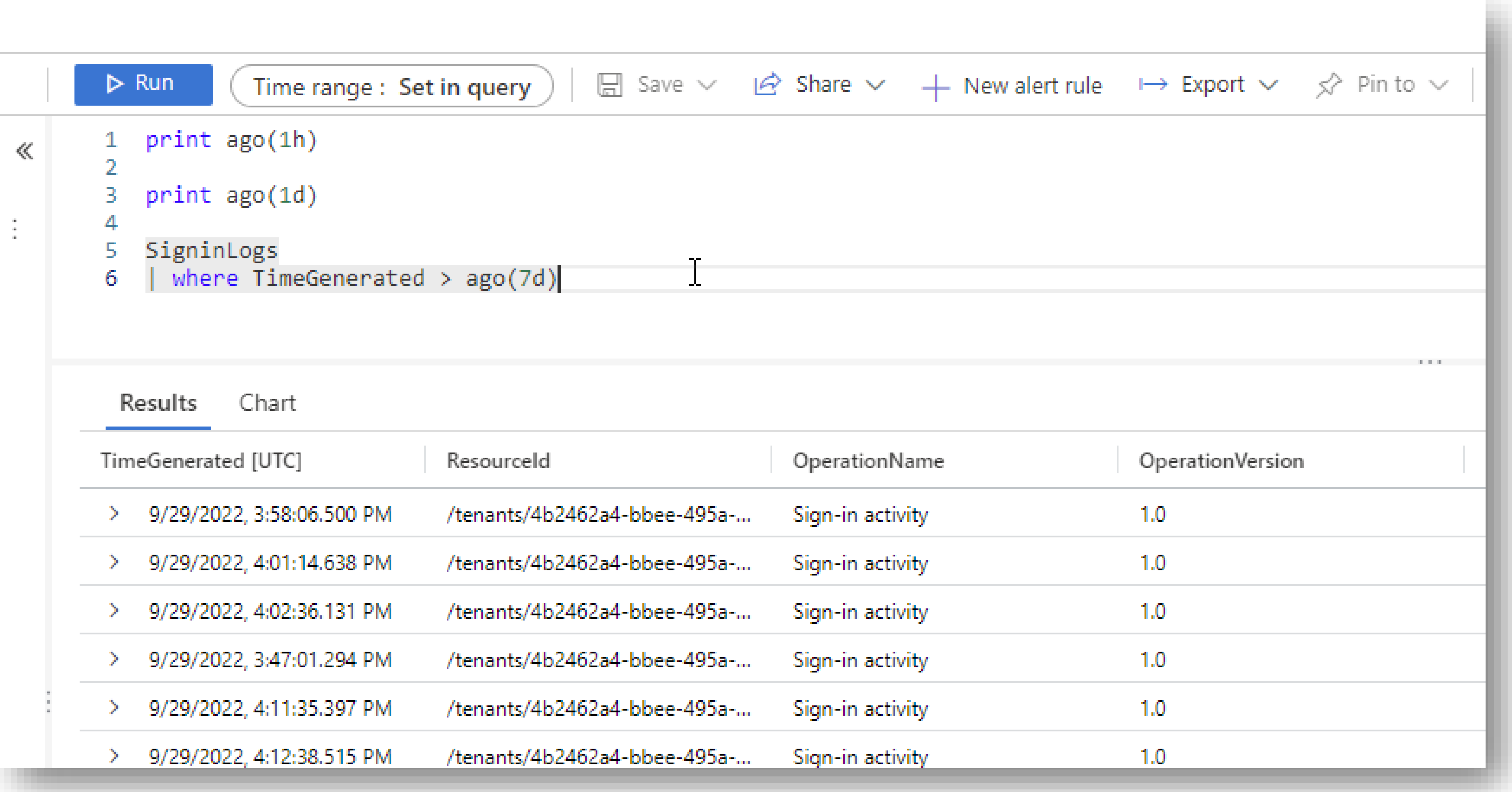
TimeGenerated [UTC]	UserPrincipalName	ClientAppUsed	AppDisplayName	IPAddress
9/28/2022, 11:28:14.078 AM	pdemo@seccxpninja.onmicros...	Browser	Microsoft Teams Web Client	188.26.211.230
9/28/2022, 11:31:18.210 AM	sync_aadcon_a5225d32ba79@s...	Mobile Apps and Desktop clients	Microsoft Azure Active Director...	40.76.220.11
9/28/2022, 11:31:23.977 AM	sync_aadcon_a5225d32ba79@s...	Mobile Apps and Desktop clients	Microsoft Azure Active Director...	40.76.220.11
9/28/2022, 11:32:28.582 AM	vijaypunja@microsoft.com	Browser	Azure Portal	86.13.181.113
9/28/2022, 11:32:56.861 AM	mthiele@microsoft.com	Browser	Microsoft 365 Security and Co...	178.1.157.49
9/28/2022, 11:34:00.147 AM	sync_dc01_3862ce34675f@secc...	Mobile Apps and Desktop clients	Microsoft Azure Active Director...	20.85.227.159
9/28/2022, 11:48:50.191 AM	viacodeteam@seccxpninja.onm...	Browser	Azure Portal	52.230.52.211
9/28/2022, 11:48:35.425 AM	sync_ninja-dc_9d913db9dfd8@...	Mobile Apps and Desktop clients	Microsoft Azure Active Director...	52.186.142.60
9/28/2022, 11:48:42.779 AM	sync_ninja-dc_9d913db9dfd8@...	Mobile Apps and Desktop clients	Microsoft Azure Active Director...	52.186.142.60
9/28/2022, 11:48:31.829 AM	csandlund@microsoft.com	Browser	Azure Portal	147.12.191.253

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/projectoperator

More Operators

KQL - ago

Subtracts the given timespan from the current UTC clock time.



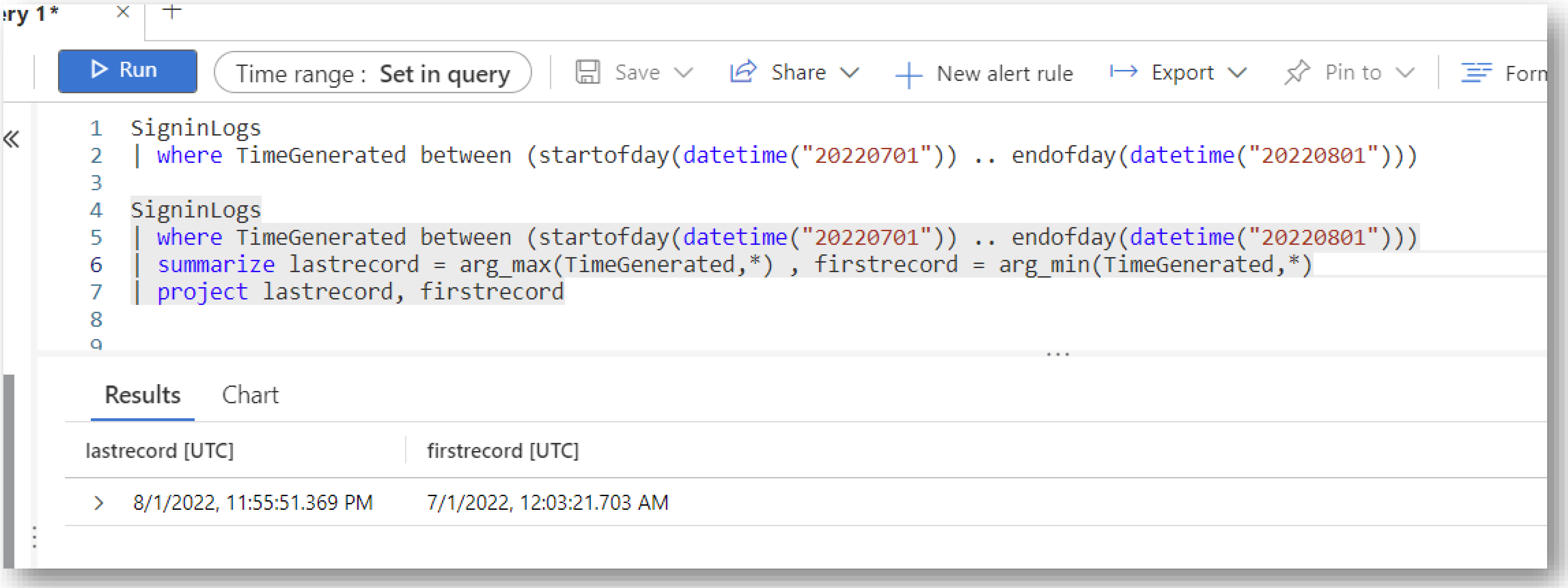
```
print ago(1h)

print ago(1d)

SigninLogs
| where TimeGenerated > ago(7d)
```

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion
9/29/2022, 3:58:06.500 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0
9/29/2022, 4:01:14.638 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0
9/29/2022, 4:02:36.131 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0
9/29/2022, 3:47:01.294 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0
9/29/2022, 4:11:35.397 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0
9/29/2022, 4:12:38.515 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/agofunction

KQL - datetime

The datetime (date) data type represents an instant in time, typically expressed as a date and time of day. Values range from 00:00:00 (midnight), January 1, 0001 Anno Domini (Common Era) through 11:59:59 P.M., December 31, 9999 A.D. (C.E.) in the Gregorian calendar.



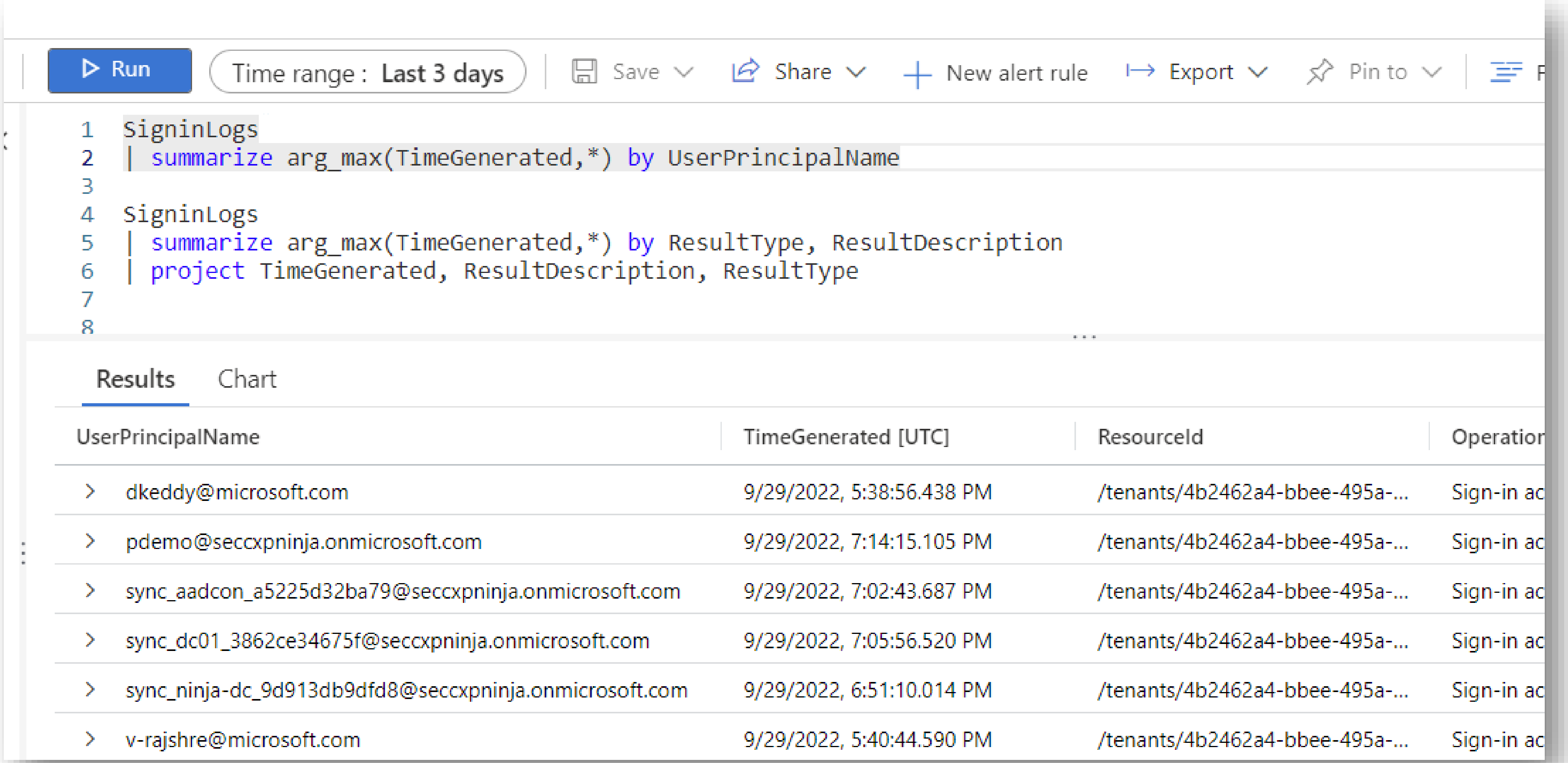
```
SigninLogs
| where TimeGenerated between (startofday(datetime("20220701")) .. endofday(datetime("20220801")))

SigninLogs
| where TimeGenerated between (startofday(datetime("20220701")) .. endofday(datetime("20220801")))
| summarize lastrecord = arg_max(TimeGenerated,*) , firstrecord = arg_min(TimeGenerated,*)
| project lastrecord, firstrecord
```

lastrecord [UTC]	firstrecord [UTC]
8/1/2022, 11:55:51.369 PM	7/1/2022, 12:03:21.703 AM

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/scalar-data-types/datetime

KQL – arg_max / arg_min

Finds a row in the group that maximizes / minimizes ExprToMaximize.



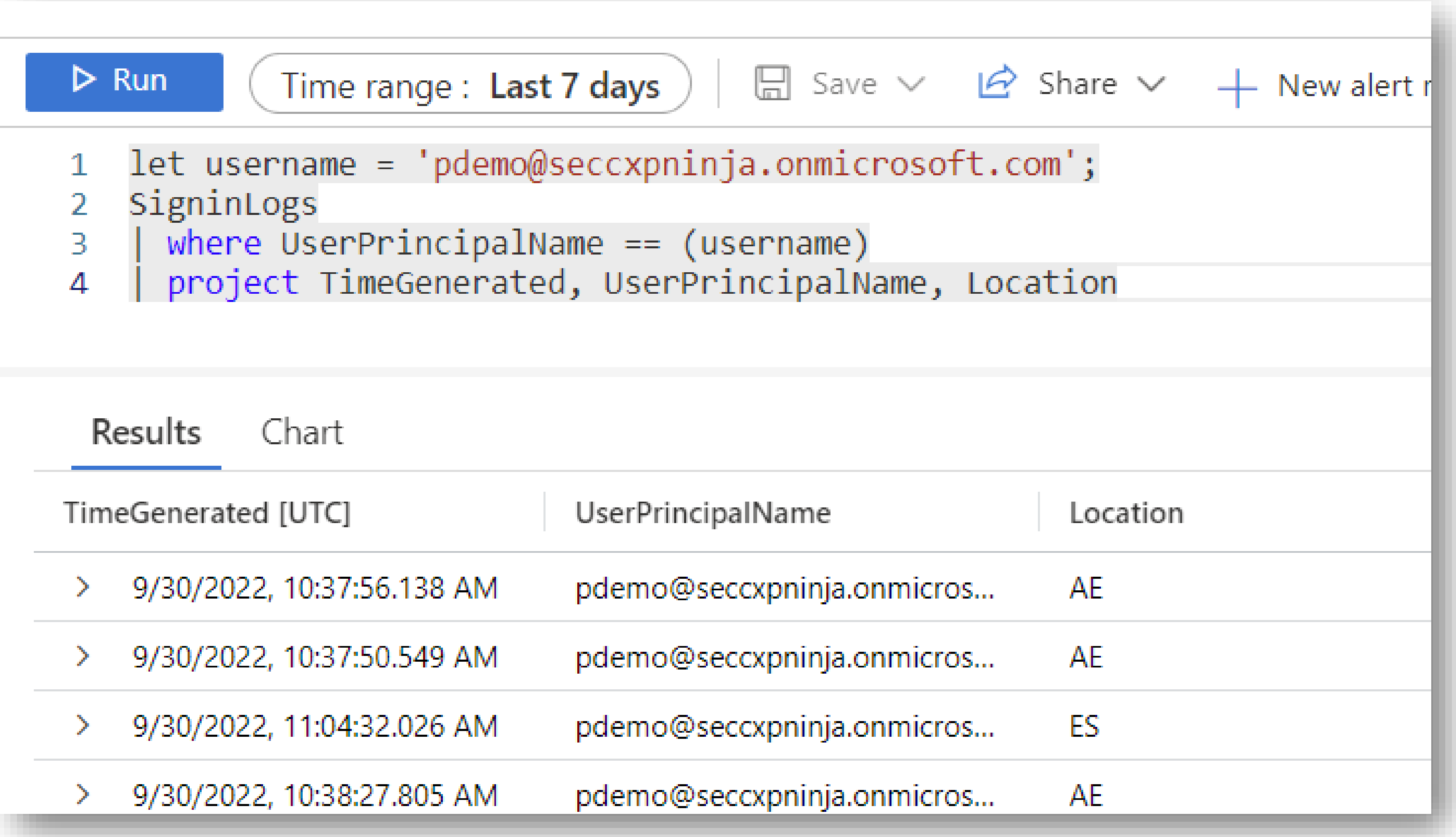
```
SigninLogs
| summarize arg_max(TimeGenerated,*) by UserPrincipalName

SigninLogs
| summarize arg_max(TimeGenerated,*) by ResultType, ResultDescription
| project TimeGenerated, ResultDescription, ResultType
```

UserPrincipalName	TimeGenerated [UTC]	ResourceId	Operatior
dkeddy@microsoft.com	9/29/2022, 5:38:56.438 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac
pdemo@seccxpninja.onmicrosoft.com	9/29/2022, 7:14:15.105 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac
sync_aadcon_a5225d32ba79@seccxpninja.onmicrosoft.com	9/29/2022, 7:02:43.687 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac
sync_dc01_3862ce34675f@seccxpninja.onmicrosoft.com	9/29/2022, 7:05:56.520 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac
sync_ninja-dc_9d913db9dfd8@seccxpninja.onmicrosoft.com	9/29/2022, 6:51:10.014 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac
v-rajshre@microsoft.com	9/29/2022, 5:40:44.590 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in ac

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/arg-max-aggfunction

KQL – let

Variable with a single value

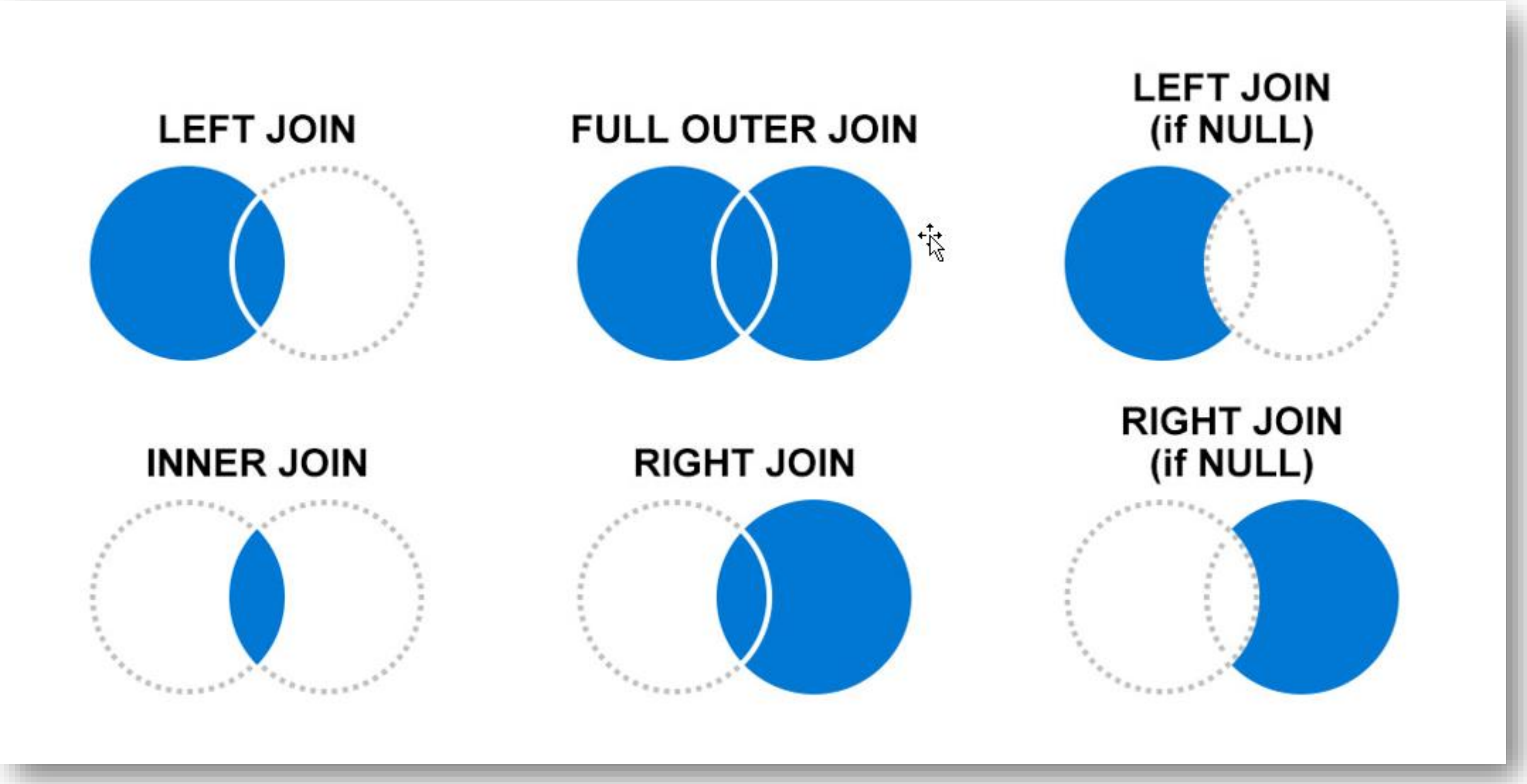


```
let username = 'pdemo@seccxpninja.onmicrosoft.com';
SigninLogs
| where UserPrincipalName == (username)
| project TimeGenerated, UserPrincipalName, Location
```

TimeGenerated [UTC]	UserPrincipalName	Location
9/30/2022, 10:37:56.138 AM	pdemo@seccxpninja.onmicros...	AE
9/30/2022, 10:37:50.549 AM	pdemo@seccxpninja.onmicros...	AE
9/30/2022, 11:04:32.026 AM	pdemo@seccxpninja.onmicros...	ES
9/30/2022, 10:38:27.805 AM	pdemo@seccxpninja.onmicros...	AE

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/letstatement

KQL – join



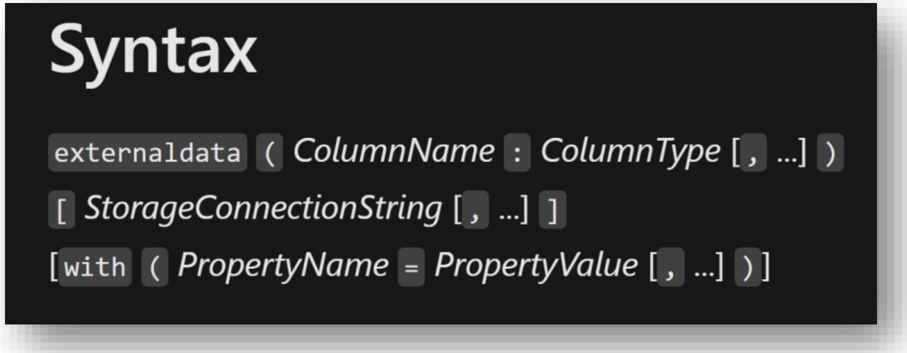
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/joinoperator?pivots=azuremonitor

KQL – join

Join Flavor	Output Records
kind=leftanti, kind=leftantisemi	Returns all the records from the left side that don't have matches from the right
kind=rightanti, kind=rightantisemi	Returns all the records from the right side that don't have matches from the left.
kind unspecified, kind=innerunique	Only one row from the left side is matched for each value of the on key. The output contains a row for each match of this row with rows from the right
kind=leftsemi	Returns all the records from the left side that have matches from the right.
kind=rightsemi	Returns all the records from the right side that have matches from the left.
kind=inner	Contains a row in the output for every combination of matching rows from left and right.
kind=leftouter (or kind=rightouter or kind=fullouter)	Contains a row for every row on the left and right, even if it has no match. The unmatched output cells contain nulls.

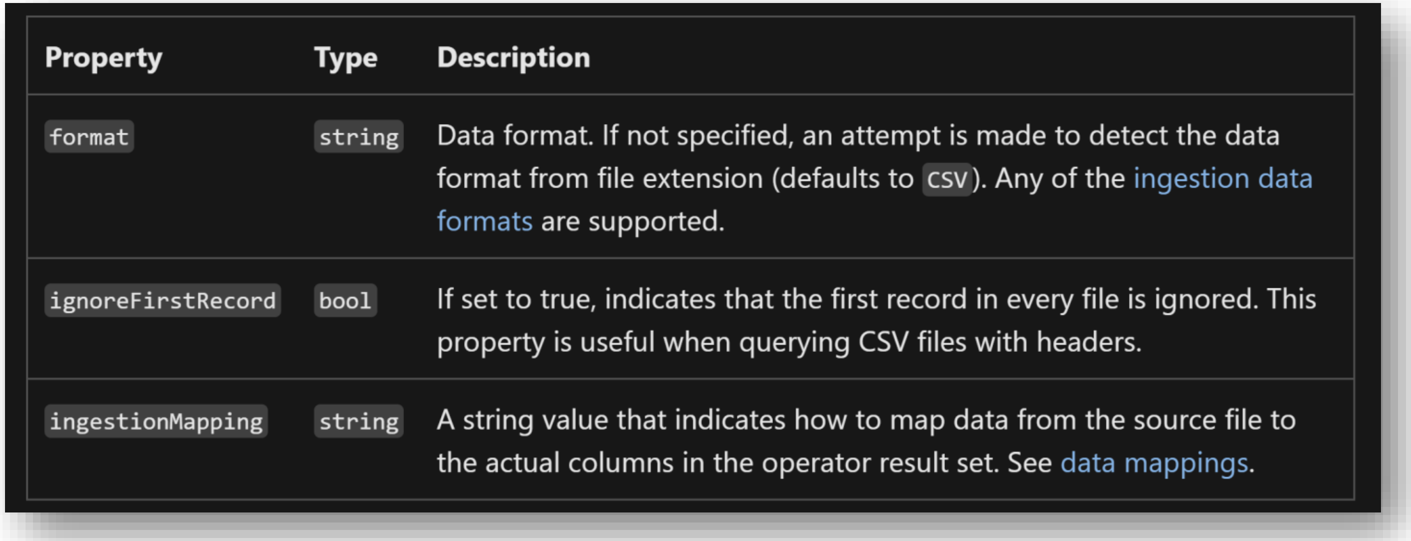
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/joinoperator?pivots=azuremonitor

KQL – externaldata

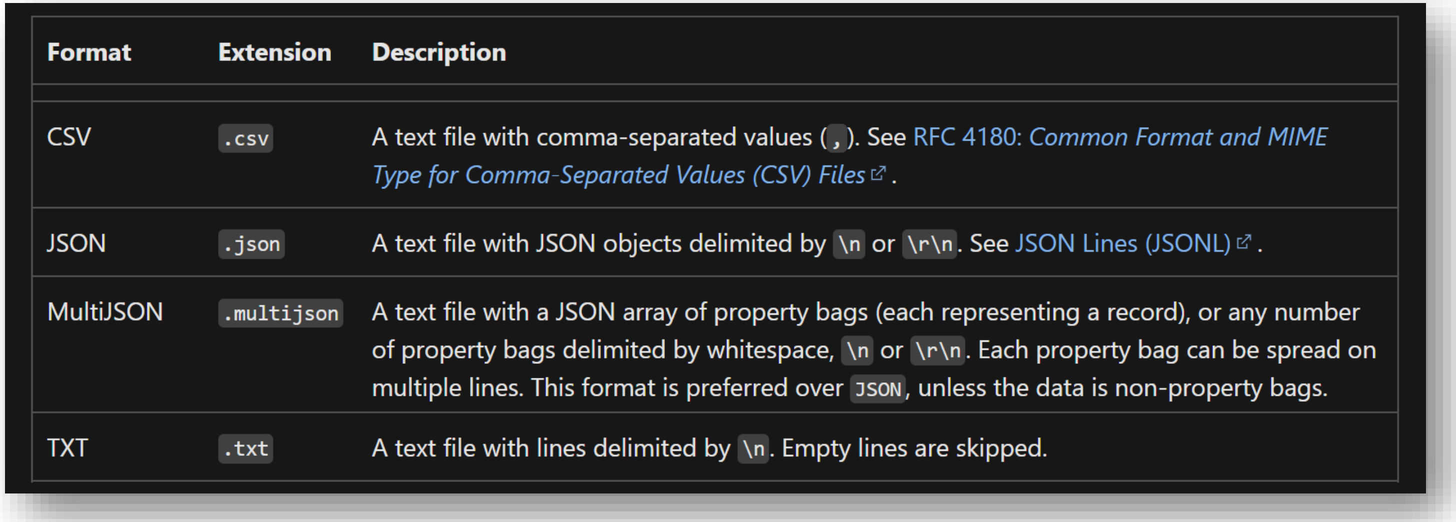


Syntax

```
externaldata ( ColumnName : ColumnType [, ...] )
[ StorageConnectionString [, ...] ]
[with ( PropertyName = PropertyValue [, ...] )]
```

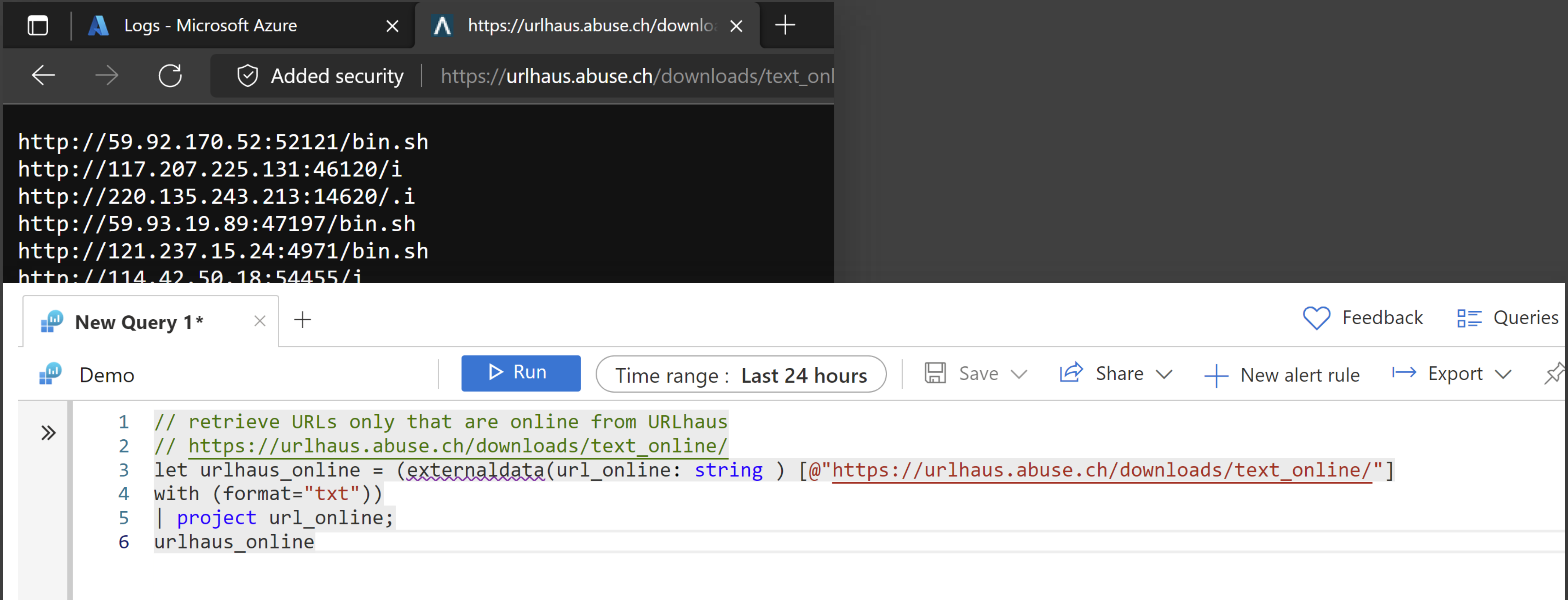


Property	Type	Description
`format`	`string`	Data format. If not specified, an attempt is made to detect the data format from file extension (defaults to `CSV`). Any of the ingestion data formats are supported.
`ignoreFirstRecord`	`bool`	If set to true, indicates that the first record in every file is ignored. This property is useful when querying CSV files with headers.
`ingestionMapping`	`string`	A string value that indicates how to map data from the source file to the actual columns in the operator result set. See data mappings.



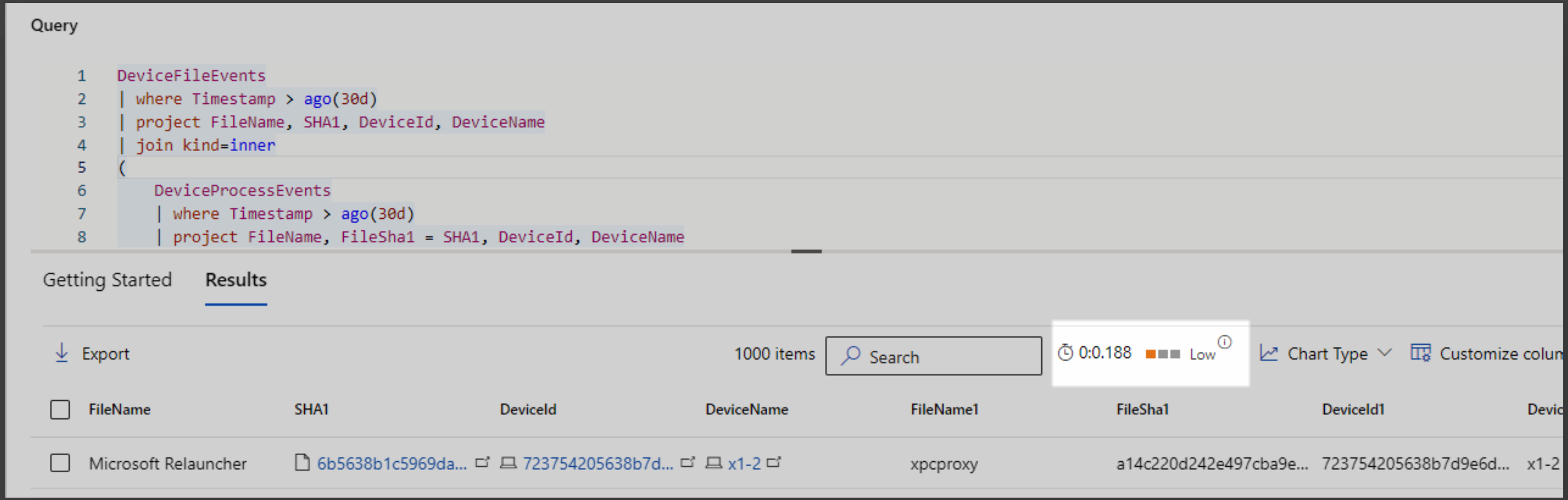
Format	Extension	Description
CSV	`.csv`	A text file with comma-separated values (`,`). See RFC 4180: *Common Format and MIME Type for Comma-Separated Values (CSV) Files* .
JSON	`.json`	A text file with JSON objects delimited by `\n` or `\r\n`. See JSON Lines (JSONL) .
MultiJSON	`.multijson`	A text file with a JSON array of property bags (each representing a record), or any number of property bags delimited by whitespace, `\n` or `\r\n`. Each property bag can be spread on multiple lines. This format is preferred over `JSON`, unless the data is non-property bags.
TXT	`.txt`	A text file with lines delimited by `\n`. Empty lines are skipped.

More ingestion formats
https://docs.microsoft.com/en-us/azure/data-explorer/ingestion-supported-formats


Logs - Microsoft Azure
https://urlhaus.abuse.ch/downlo
Added security
https://urlhaus.abuse.ch/downloads/text_onl
New Query 1*
Feedback
Queries
Demo
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export

```
http://59.92.170.52:52121/bin.sh
http://117.207.225.131:46120/i
http://220.135.243.213:14620/.i
http://59.93.19.89:47197/bin.sh
http://121.237.15.24:4971/bin.sh
http://114.42.50.18:54455/i
```

```
// retrieve URLs only that are online from URLhaus
// https://urlhaus.abuse.ch/downloads/text_online/
let urlhaus_online = (externaldata(url_online: string ) [@"https://urlhaus.abuse.ch/downloads/text_online/"]
with (format="txt"))
| project url_online;
urlhaus_online
```



Query

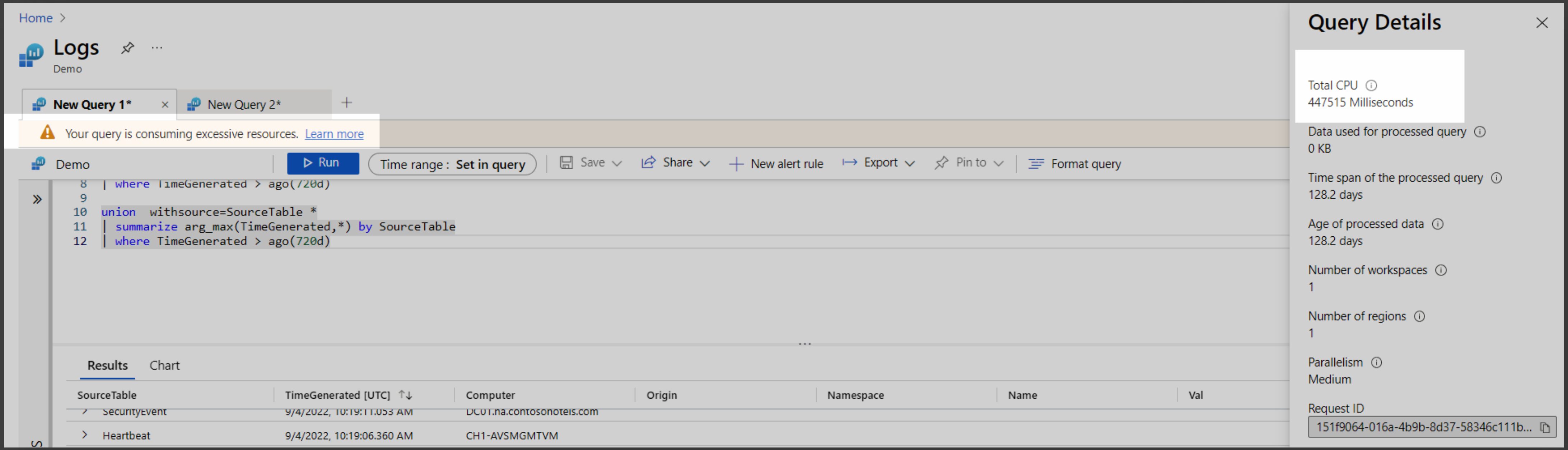
```
DeviceFileEvents
| where Timestamp > ago(30d)
| project FileName, SHA1, DeviceId, DeviceName
| join kind=inner
(
    DeviceProcessEvents
    | where Timestamp > ago(30d)
    | project FileName, FileSha1 = SHA1, DeviceId, DeviceName
```

1000 items

0:0.188 Low

FileName	SHA1	DeviceId	DeviceName	FileName1	FileSha1	DeviceId1	Devic
Microsoft Relauncher	6b5638b1c5969da...	723754205638b7d...	x1-2	xpcproxy	a14c220d242e497cba9e...	723754205638b7d9e6d...	x1-2

Query that utilizes more than 100 seconds of CPU is considered a query that consumes excessive resources. Query that utilizes more than 1,000 seconds of CPU is considered an abusive query and might be throttled.



⚠ Your query is consuming excessive resources. Learn more

Time range : Set in query

```
| where TimeGenerated > ago(720d)

union  withsource=SourceTable *
| summarize arg_max(TimeGenerated,*) by SourceTable
| where TimeGenerated > ago(720d)
```

SourceTable	TimeGenerated [UTC]	Computer	Origin	Namespace	Name	Val
SecurityEvent	9/4/2022, 10:19:11.053 AM	DC01.na.contosohotels.com				
Heartbeat	9/4/2022, 10:19:06.360 AM	CH1-AVSMGMTVM				

Query Details

Total CPU ⓘ
447515 Milliseconds

Data used for processed query ⓘ
0 KB

Time span of the processed query ⓘ
128.2 days

Age of processed data ⓘ
128.2 days

Number of workspaces ⓘ
1

Number of regions ⓘ
1

Parallelism ⓘ
Medium

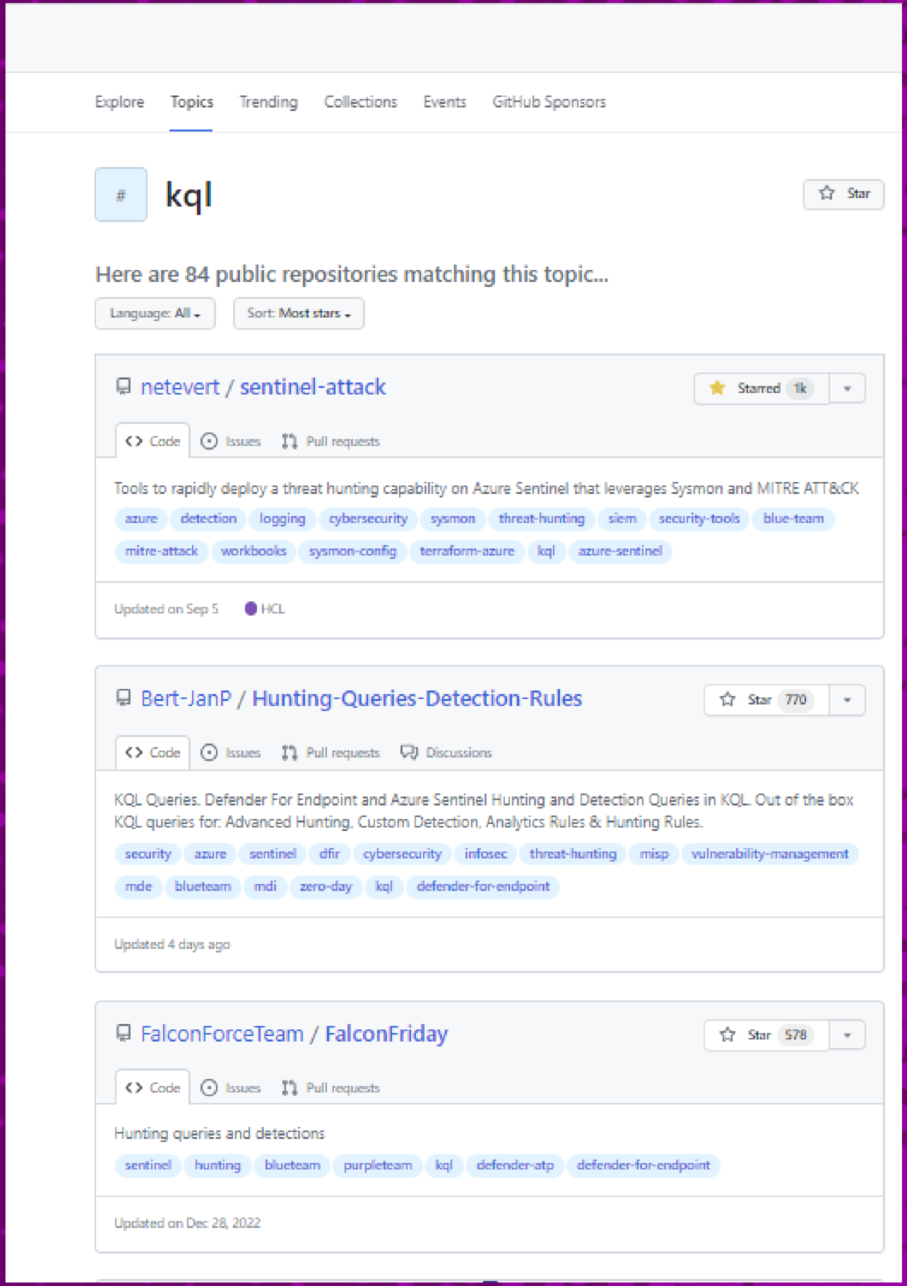
Request ID
151f9064-016a-4b9b-8d37-58346c111b...

geekmania

KQL

- Learn from Others
- Learn by yourself

GitHub



kql

Here are 84 public repositories matching this topic...

Language: All
Sort: Most stars

netevert / sentinel-attack

Tools to rapidly deploy a threat hunting capability on Azure Sentinel that leverages Sysmon and MITRE ATT&CK

azure detection logging cybersecurity sysmon threat-hunting siem security-tools blue-team mitre-attack workbooks sysmon-config terraform-azure kql azure-sentinel

Updated on Sep 5 ● HCL

Bert-JanP / Hunting-Queries-Detection-Rules

KQL Queries. Defender For Endpoint and Azure Sentinel Hunting and Detection Queries in KQL. Out of the box KQL queries for: Advanced Hunting, Custom Detection, Analytics Rules & Hunting Rules.

security azure sentinel dfir cybersecurity infosec threat-hunting misp vulnerability-management mde blueteam mdi zero-day kql defender-for-endpoint

Updated 4 days ago

FalconForceTeam / FalconFriday

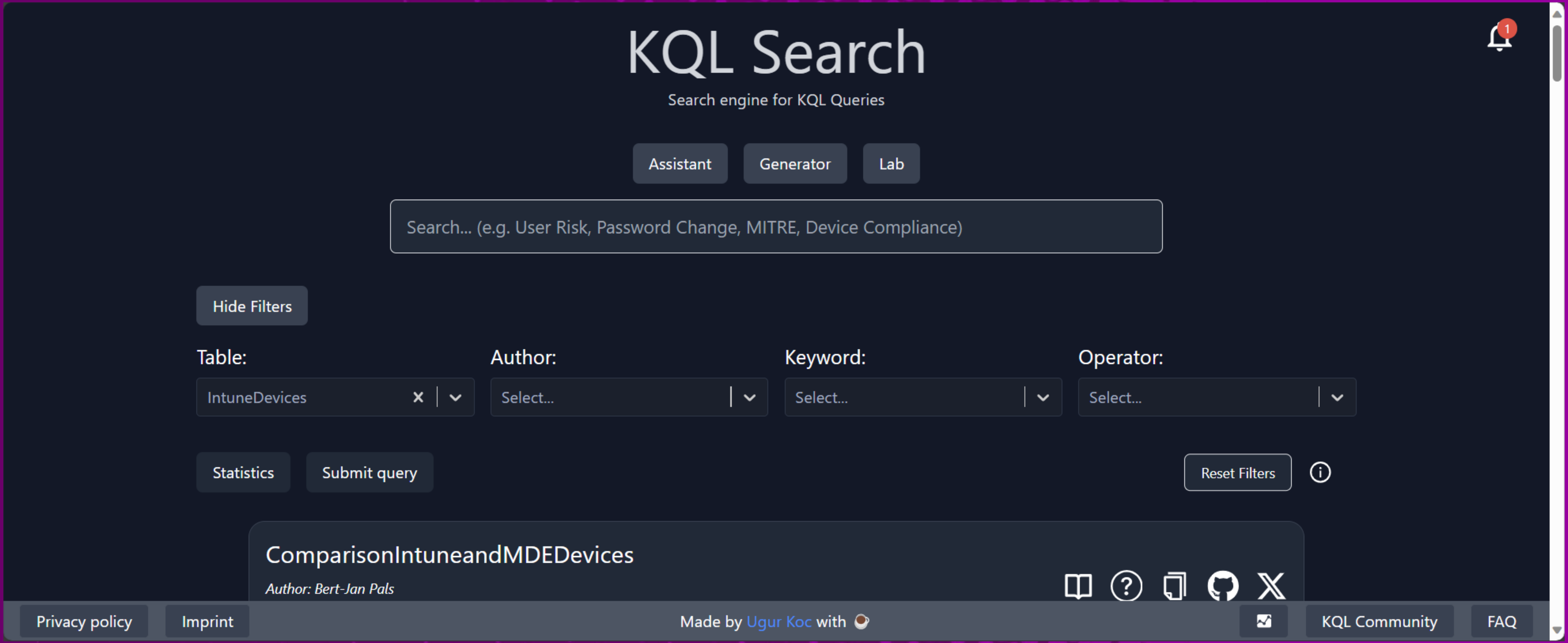
Hunting queries and detections

sentinel hunting blueteam purpleteam kql defender-atp defender-for-endpoint

Updated on Dec 28, 2022

geekmania

KQL Search – Your Best Friend



KQL Search

Search engine for KQL Queries

Search... (e.g. User Risk, Password Change, MITRE, Device Compliance)

Table: IntuneDevices

Author: Select...

Keyword: Select...

Operator: Select...

ComparisonIntuneandMDEDevices

Author: Bert-Jan Pals

geekmania

KQL|Cafe

More KQL Learning Resources

Must Learn KQL	https://aka.ms/MustLearnKQL
KQL Café	https://kqlcafe.com
KQL Search	https://kqlsearch.com
KQL Query	https://kqlquery.com
The KQL Mysteries	https://github.com/rod-trent/KQLMysteries
Kusto Detective Agency	https://detective.kusto.io/

MUST LEARN KQL

geekmania