Damien Van Robaeys

Modern Workplace consultant & MVP

MODERN ENDPOINT MANAGEMENT SUMMIT 2023 EMEA EDITION

Getting started with Log Analytics & Intune reporting

6th-7th september

@syst_and_deploy

Thank you!!

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

SILVER SPONSOR

PATCH MY PC

Rimo3

METSYS

MODERN ENDPOINT MANAGEMENT SUMMIT 2023 EMEA EDITION

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

GOLD SPONSOR

Microsoft

DELL Technologies

6th-7th september

Slides and demos

@syst_and_deploy #MEMSummit

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Slides & demos are already available

https://github.com/damienvanrobaeys/Events_Slides

SCAN ME

SCHED

What you will learn here ?

@syst_and_deploy #MEMSummit

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

1 **Existing reports**

2 **What it Log Analytics**

2 **KQL fundamentals**

3 **Sending custom data (2 ways)**

4 **Creating a fake data lab**

5 **Creating workbook in live**

Custom reports we will see

@syst_and_deploy #MEMSummit

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Monitor BSOD (blue screen)

A dashboard allowing you to troubleshoot BSOD on your devices

Available on my blog
Link here

Drivers inventory

A dashboard allowing you to see all drivers installed on all devices

Available on my blog
Link here

Monitor applications on devices

A solution to send Intune discovered apps to log analytics

Available on my blog
Link here

A bit about me

@syst_and_deploy #MEMSummit

Modern Workplace consultant (Metsys) & MVP Microsoft (7 years).
Working with PowerShell, Intune, MS Graph, MECM, Log Analytics…

systanddeploy.com

@syst_and_deploy

damien.vanrobaeys@gmail.com

Damien Van Robaeys

Microsoft Most Valuable Professional Award

METSYS

systanddeploy.com

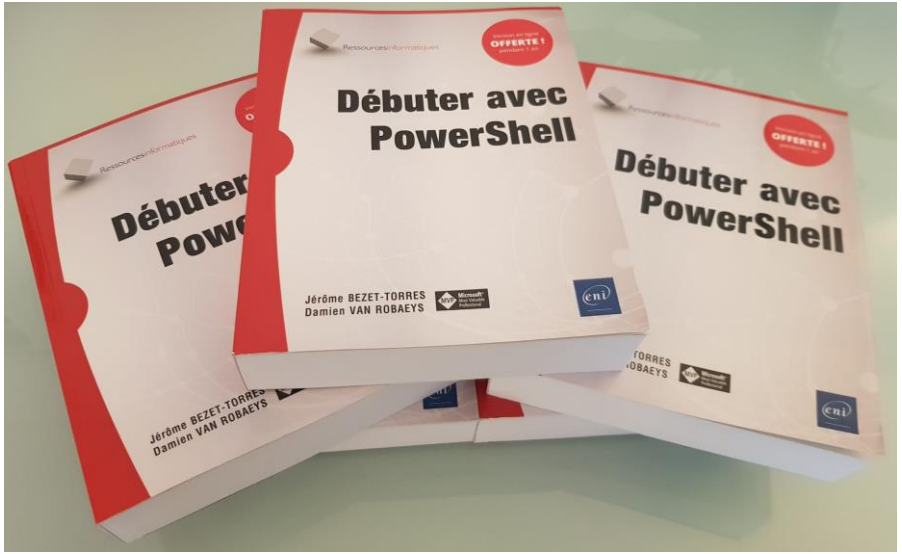
Win my book (in French)

@syst_and_deploy #MEMSummit

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Win my book today & tomorrow

ℹ Book in French



A question ?

@syst_and_deploy #MEMSummit

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Time is limited, ask me at the end of the session

Existing reporting solutions

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Existing reports in Intune

- Many reports for devices, applications, group policy analytics, updates…
- Devices: assignment failures, autopilot deployment, update reports…
- Apps: discovered apps, device apps status…

Device management

- Device compliance
- Device configuration (preview)
- Group policy analytics (preview)
- Windows updates (preview)
- Cloud attached devices (preview)

Reports

- Startup performance
- Proactive remediations
- Recommended software
- Application reliability
- Work from anywhere (preview)

Antivirus agent status

See the agent status of your devices. Shows which devices have real-time or network protection and their state.

Detected malware

See the malware state of your devices. Shows the number of devices with detected malware and malware details.

Intune data warehouse and Power BI

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

What are benefits ?

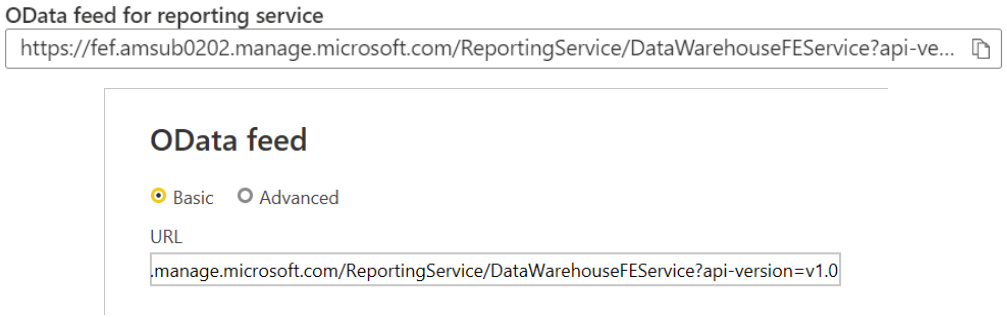
- More information than Azure portal
- You can access to historical Intune data
- Data refreshed on a daily cadence

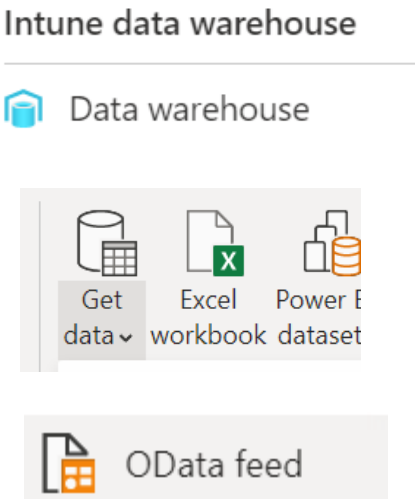
Where ?

- **Report** > **Intune data warehouse** > **Data warehouse**

How to connect ?

- **Get data** > **OData feed** > type OData feed link





Demo: existing reports

What will we see ?

- Intune Data Wharehouse

What is Log Analytics ?

MODERN
ENDPOINT
MANAGEMENT
SUMMIT 2023

Starting with Log Analytics series

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Blog post series about starting with Log Analytics

https://www.systanddeploy.com/search/label/LogAnalytics_Start

1. Creating our first Log Analytics workspace
2. Importing your own data into the workspace
3. Creating our first workbook
4. Add Intune data into Log Analytics workspace
5. Running KQL queries in Log Analytics with PowerShell
6. Creating a lab by importing a CSV with fake data
7. Give your workbook a better look
8. Sending data to Log Analytics from Azure Automation
9. Sending data from Log Analytics to Power BI

SCAN ME

What is Log Analytics ?

- Part of Azure available from Azure & Intune portals
- Run queries and play with data from your tenant, devices…
- Data are located into Logs

By default, Log Analytics is empty you need to configure it

Log Analytics prerequisites

1. Azure subscription (of course)
2. Resource group (container that holds all your resources) *
3. Log Analytics workspace (we will see this later)

* More info about resource group

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal

Log Analytics Workspace

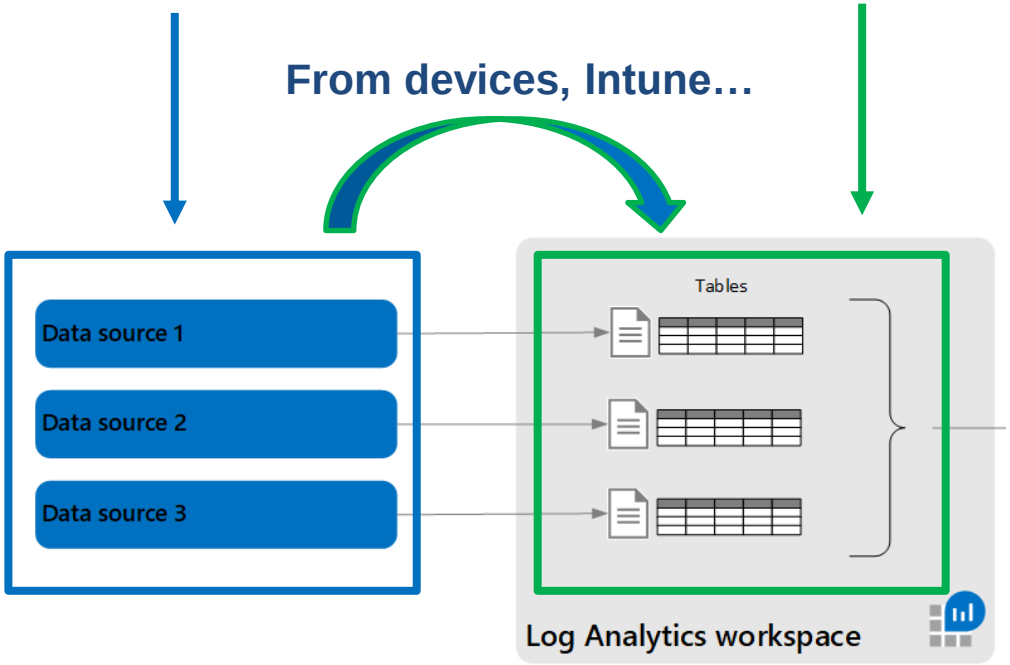
- A workspace has a unique ID* and resource ID
- When you collect logs, all data are stored in a workspace

** We will use the Workspace ID to send custom data later in the session*

- Contains all things relative to your logs and data:
  - ✓ Logs, Custom log
  - ✓ Microsoft Sentinel, Microsoft Defender portal

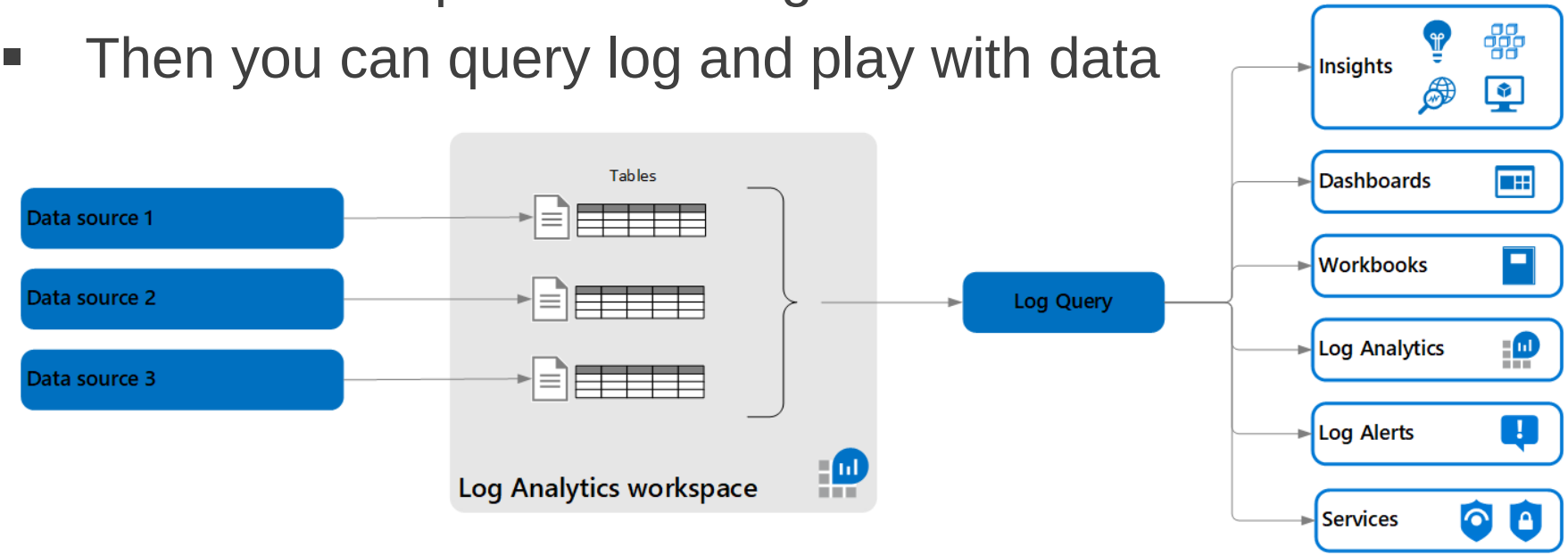
Data structure

- Data are sent from a source in Tables in a Workspace



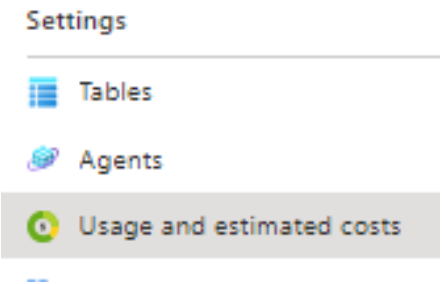
Data structure

- Tables organized in columns containing rows of data
- A table corresponds to a Log
- Then you can query log and play with data



Log Analytics and pricing

- Log Analytics is **priced/billed by ingestion and retention**
- The default pricing for Log Analytics is a pay-as-you-go
- Default pricing (get it through the portal):
  - ✓ Ingestion: €2,532/GB
  - ✓ Retention: €0,12/GB
- For more info go to: **Usage and estimated costs**



Log Analytics and pricing: useful KQL

- Useful table to analyze data & usage: **Usage** (in LogManagement)
- Use property: **IsBillable == true**
- Query to get billable data volume by type over the last day

```
Usage
| where TimeGenerated > ago(1d)
| where IsBillable == true
| where Solution contains "LogManagement"
| summarize BillableDataGB = sum(Quantity) / 1000. by bin(StartTime, 1d), DataType
| order by BillableDataGB
```

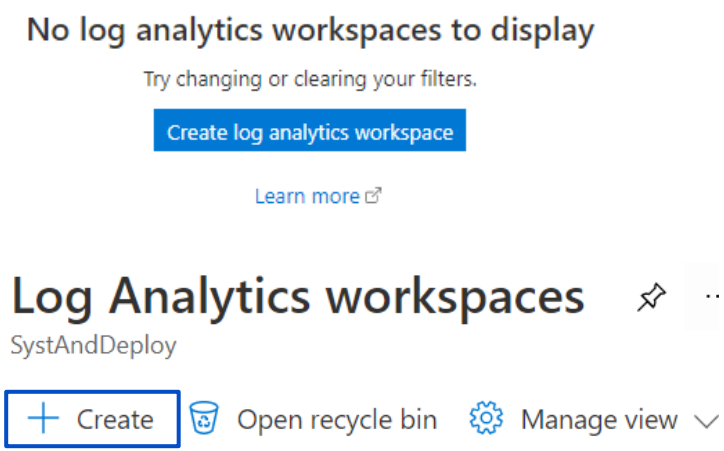
* More info: https://mlaraib-khan.medium.com/analyze-usage-and-cost-in-log-analytics-ms-azure-774d27127aed

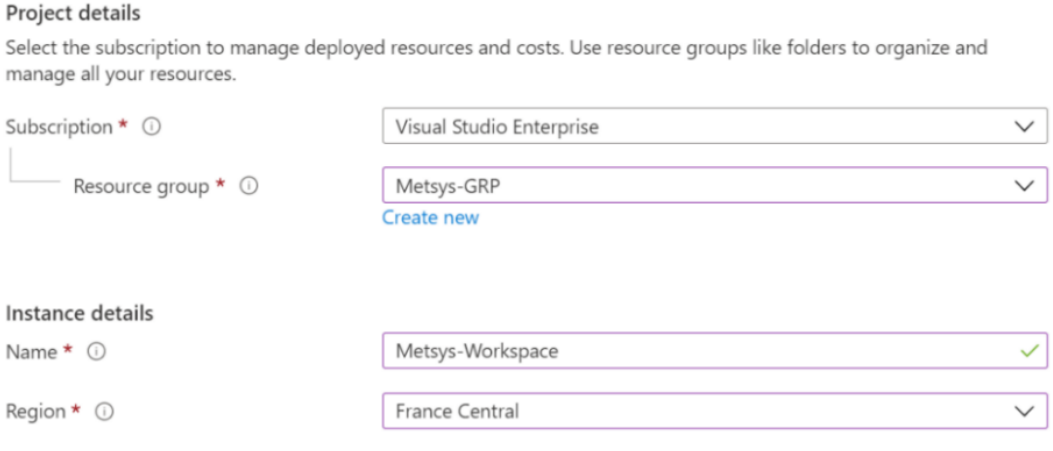
Creating a workspace

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Manually

1. Go to **Log Analytics workspaces** > **Create**
2. Fill information



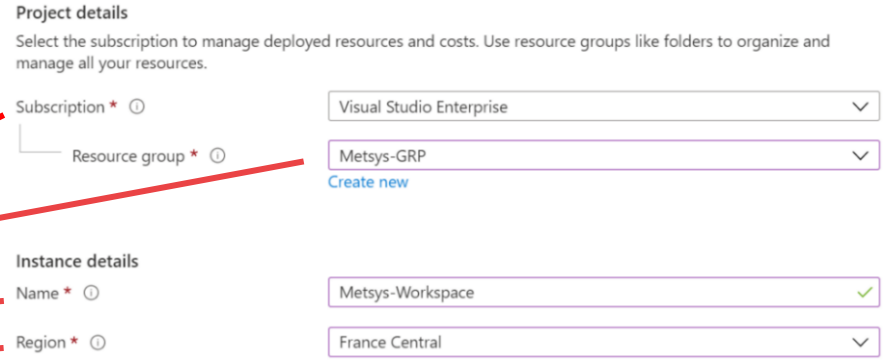


Creating a workspace

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

With PowerShell

1. Install module **Az**: Install-Module -Name Az -Force
2. Connect-AzAccount
3. New-AzOperationnalInsightsWorkspace



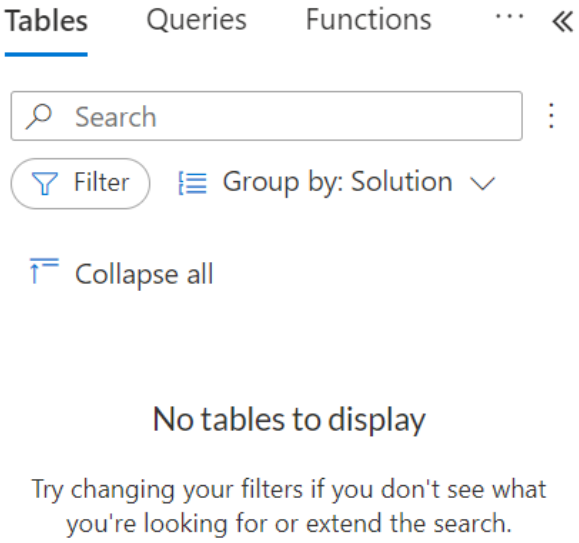

```
$SubscriptionID = "Your subscription"
$ResourceGroup = "Metsys-GRP"
$WorkspaceName = "Metsys-Workspace"
$Location = "francecentral"

Connect-AzAccount -Subscription $SubscriptionID
New-AzOperationalInsightsWorkspace -Location $Location -Name $WorkspaceName -ResourceGroupName $ResourceGroup
```

Adding Intune data to your workspace

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

By default Logs part is empty (no tables)

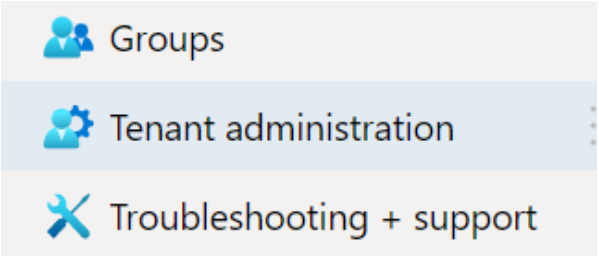
First step: add Intune datas to Log Analytics workspace

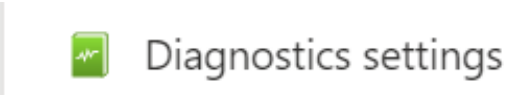


Adding Intune data to your workspace

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

- Go to **Intune** > **Tenant administration** > **Diagnostic settings**
- Click on **Add diagnostic setting**





Diagnostic settings

Name	Storage account	Event hub	Log Analytics works...
Intune	-	-	damien
IntuneLogs	-	-	metsys-workspace

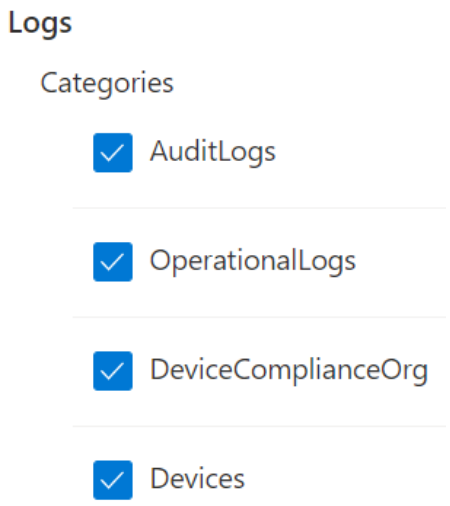
+ Add diagnostic setting

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

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices

Intune logs

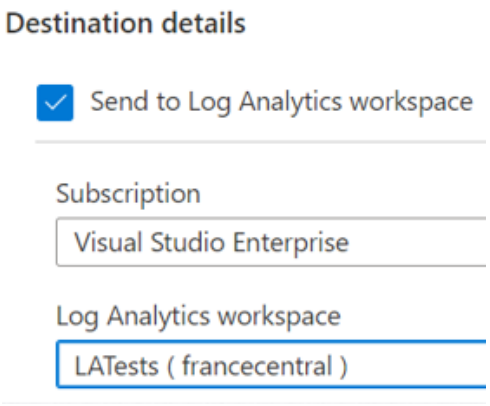
- Select built-in logs to add



- **AuditLogs**: activities record that generate a change in Intune Intune (including create, update, delete, assign, and remote actions)
- **OperationalLogs**: details about users and devices that successfully enrolled (or failed) to enroll and details on non-compliant devices
- **DeviceComplianceOrg**: Contains report for device compliance in Intune and details on non-compliant devices
- **Devices**: device inventory and status information about Intune enrolled and managed devices

Intune logs

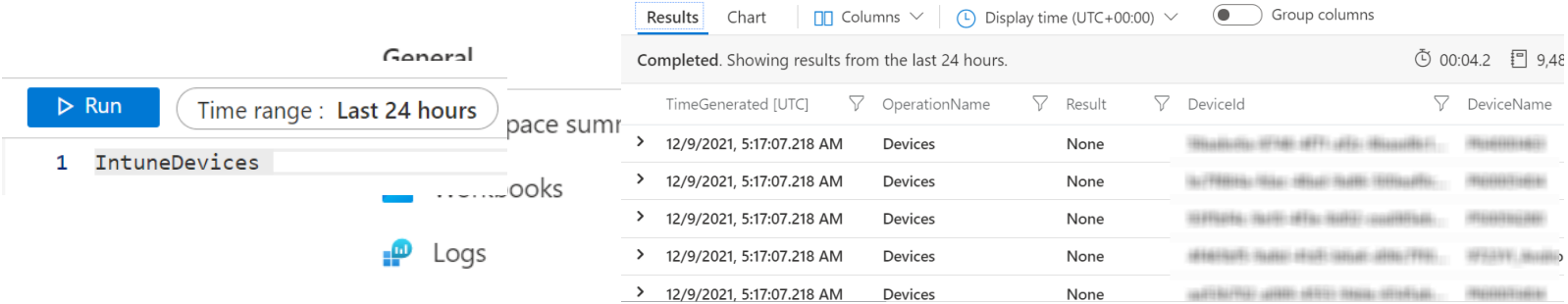
- Select workspace where to send data



- **AuditLogs**: activities record that generate a change in Intune Intune (including create, update, delete, assign, and remote actions)
- **OperationalLogs**: details about users and devices that successfully enrolled (or failed) to enroll and details on non-compliant devices
- **DeviceComplianceOrg**: Contains report for device compliance in Intune and details on non-compliant devices
- **Devices**: device inventory and status information about Intune enrolled and managed devices

Log Analytics & Intune

- Go to **Logs**
- You have now Intune logs
  - Example **IntuneDevices** (list enrolled devices)
- You can now run query on your Intune datas
- Language for query is **KQL** (Kusto Query Language)



Demo: first overview

What will we see ?

- Workspace overview
- Data structure, logs…
- Playing with Intune table

KQL (Kusto Query Language)

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

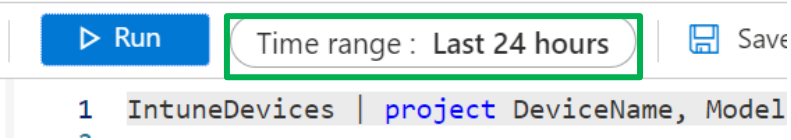
KQL, the heart of your analysis

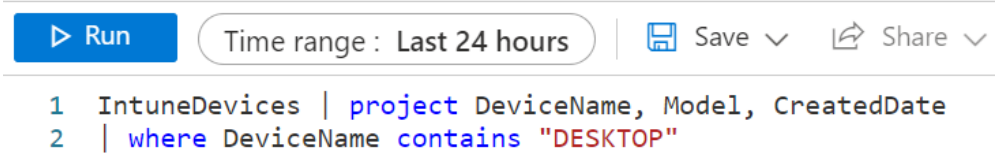
- KQL for **Kusto Query Language**
- Language to request/explore data from your Logs
- Same language than in CMPivot
- Structure is similar than in SQL: tables, columns…
- Used in Log Analytics, Sentinel, M365 Defender…

Starting with KQL

1. Select a log like **IntuneDevices**
2. Select a **time range**
3. Use pipe **|** delimiter with **where** operator (there are essentials)

- **| where** : allows you to filter on a field (***contains***, ***==***, ***startswith…)***
- **| project** operator : allow you to select fields (columns) to display
- isnotempty(column), | join, | order, | count, | top, ago(delay)





KQL cheat sheets

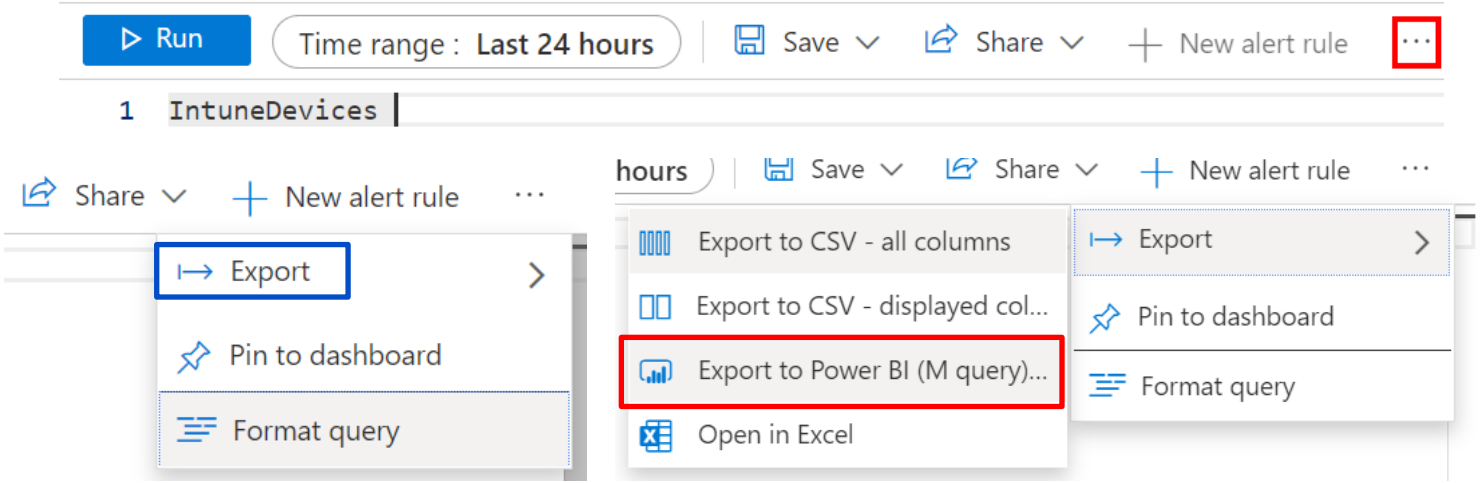
MODERN ENDPOINT MANAGEMENT SUMMIT 2023

An easy way to start with KQL

https://techcommunity.microsoft.com/t5/azure-data-explorer-blog/azure-data-explorer-kql-cheat-sheets/ba-p/1057404

Log Analytics from Power BI ?

- You can create a query in LA and use it in Power BI
- Go to … > **Export** > **Export to PBI (M query)**



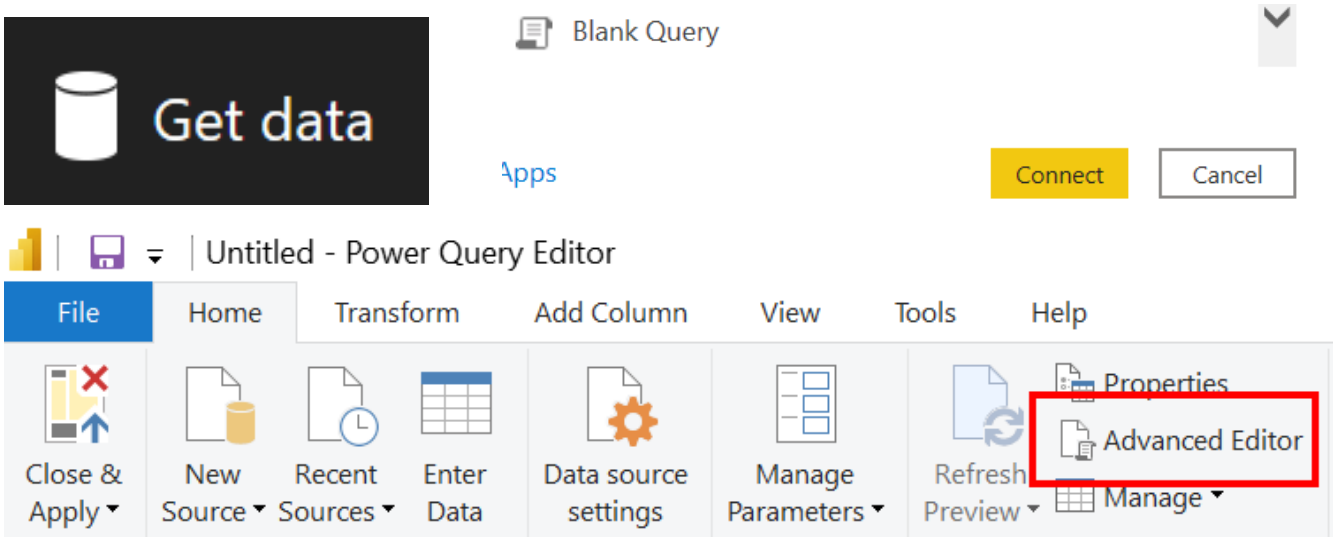
Log Analytics from Power BI ?

- Copy file content

```
let AnalyticsQuery =
let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/
[Query=[#"query"="IntuneDevices | project DeviceName, DeviceId, UPN, OSVersion, Mod
",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="P1D",#"prefer"="ai.response-thinning=t
TypeMap = #table(
{ "AnalyticsTypes", "Type" },
{
{ "string",   Text.Type },
{ "int",      Int32.Type },
{ "long",     Int64.Type },
{ "real",     Double.Type },
{ "timespan", Duration.Type },
{ "datetime", DateTimeZone.Type },
{ "bool",     Logical.Type },
{ "guid",     Text.Type },
{ "dynamic",  Text.Type }
}),
DataTable = Source[tables]{0},
```

Log Analytics from Power BI ?

- In PBI go to **Get data** > **Blank query** > **Connect** > **Advanced editor**



Log Analytics from Power BI ?

- Replace content from Query1 with file content

```
let AnalyticsQuery =
let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/
[Query=[#"query"="IntuneDevices | project DeviceName, DeviceId, UPN, OSVersion, Mod
",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="P1D",#"prefer"="ai.response-thinning=t
TypeMap = #table(
{ "AnalyticsTypes", "Type" },
{
{ "string",   Text.Type },
{ "int",      Int32.Type },
{ "long",     Int64.Type },
{ "real",     Double.Type },
{ "timespan", Duration.Type },
{ "datetime", DateTimeZone.Type },
{ "bool",     Logical.Type },
{ "guid",     Text.Type },
{ "dynamic",  Text.Type }
}),
DataTable = Source[tables]{0},
```

Query1

```
let
    Source = ""
in
    Source
```

Demo: let’s start with KQL

What will we see ?

- Understanding KQL
- Quick start with basic queries

Custom reporting

MODERN
ENDPOINT
MANAGEMENT
SUMMIT 2023

How does it work ?

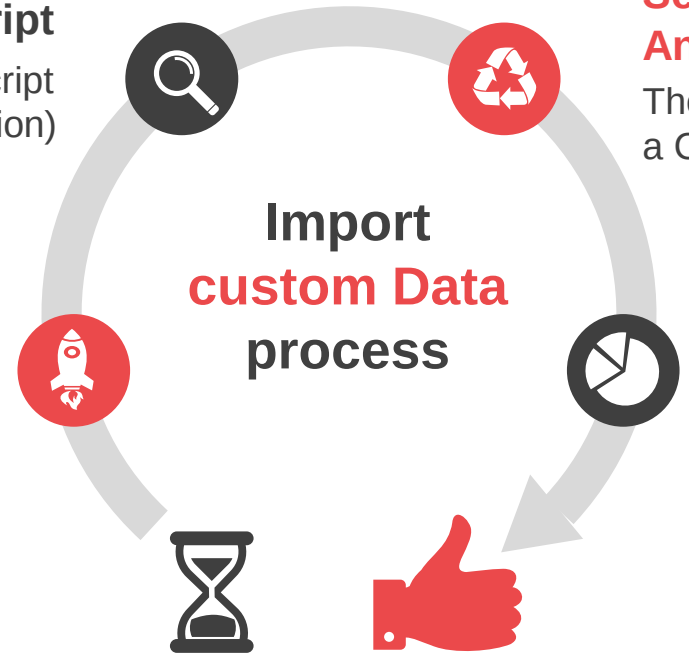
MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Scheduling the script

Add & schedule the script (Remediation or Azure Automation)

Sending data to Log Analytics

The script will send them into a Custom Log in Log Analytics



Creating a script to get data

Create a script to get data you want from devices or tenant

Gather data in a report

Once data are in the Custom Log, we can create a workbook with them

Azure Monitor HTTP Data Collector API

- **What ?** Used to send custom data to a Workspace
- **From where ?** From any clients that can call a REST API
- **How ?** POST request with data in JSON format

* More info here

Sending data with PowerShell

Functions **Build-Signature** and **Post-LogAnalyticsData**

- Build-Signature: getting token
- Post-LogAnalyticsData: sending data to LA

* MS functions, more info here

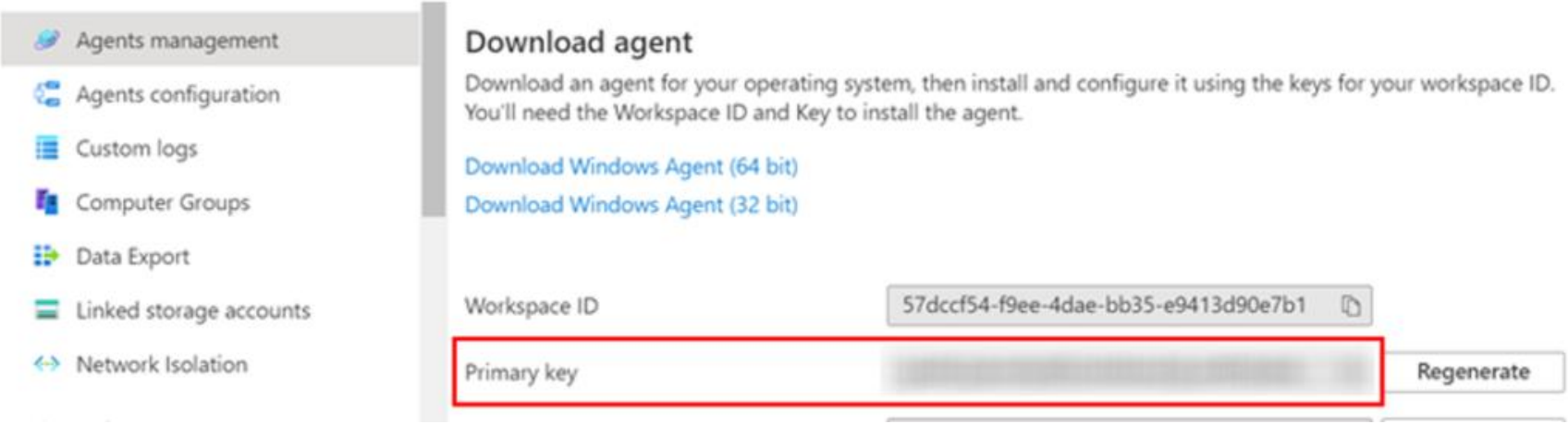
Required information (for sending data)

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Info required to import data through a script into Log Analytics:

- **$CustomerId**: Log Analytics Workspace ID
- **SharedKey**: Primary Key
- **$LogType**: Name of the Custom Log to create or update

Used as credentials



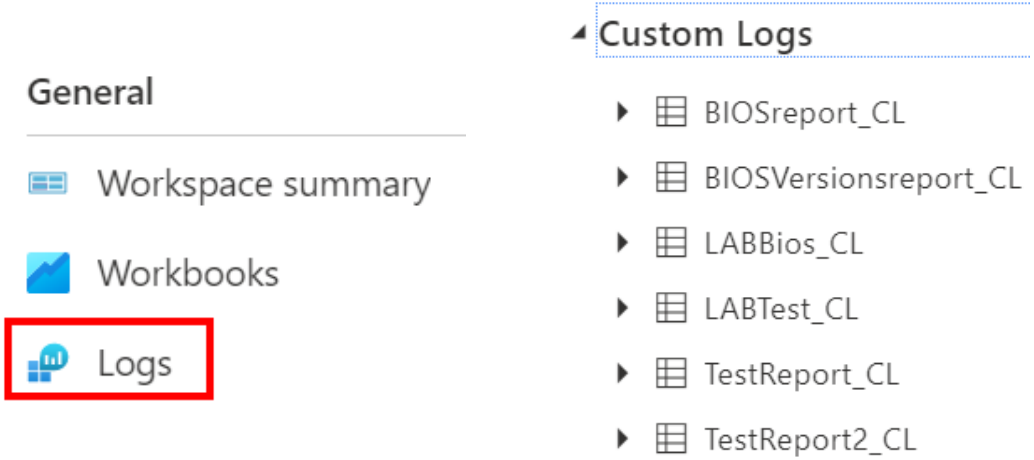
Sending data ? From where ?

1. **Remediation script:** to import data from devices
   - Local admin report
   - Drivers inventory
   - BIOS versions report
   - Disk size report

2. **Azure Automation runbook:** send data from your environment
   - BSOD report
   - Discovered apps dashboard

Custom data in Log Analytics

- Located in **Logs** > **Custom Logs**
- Custom Log named like: **YourCustomLog _CL**



Sending data with Remediation script

1. Use MS functions (mentioned before)
2. Collect data to send in Log Analytics in array
3. Convert data to JSON
4. Send data with **Post-LogAnalyticsData** function

```
$Properties = [Ordered] @{
    "Device" = $env:computername
    "ModelFriendlyName" = (gwmi win32_computersystem).SystemFamily
    "ModelMTM" = ((gwmi win32_computersystem).Model).Substring(0,4)
    "Uptime" = Get_DeviceUpTime -Show_Uptime
    "BIOSDate" = (gwmi win32_bios | select *).ReleaseDate
    "FullBiosVersion" = (gwmi win32_bios).SMBIOSBIOSVersion
}
$Infos = New-Object -TypeName "PSObject" -Property $Properties
```

Sending data with Remediation script

1. Use MS functions (mentioned before)
2. Collect data to send in Log Analytics in array
3. Convert data to JSON
4. Send data with **Post-LogAnalyticsData** function

```
$InfosJson = $Infos | ConvertTo-Json
$params = @{
    CustomerId = $customerId
    SharedKey  = $sharedKey
    Body       = ([System.Text.Encoding]::UTF8.GetBytes($InfosJson))
    LogType    = $LogType
}
$LogResponse = Post-LogAnalyticsData @params
```

Sending data with Azure Automation

1. Configure Azure Automation with a managed identity*
2. Create a Runbook in Azure Automation
3. Authenticate to your tenant with the managed identity*
4. Use both MS functions (mentioned before)
5. Use MS Graph to collect data
6. Convert data to JSON
7. Send data with **Post-LogAnalyticsData** function

* More info: https://learn.microsoft.com/en-us/azure/automation/enable-managed-identity-for-automation

Managed identities: what is it ?

- When you create scripts, you must deal with credentials, secrets, certificates…

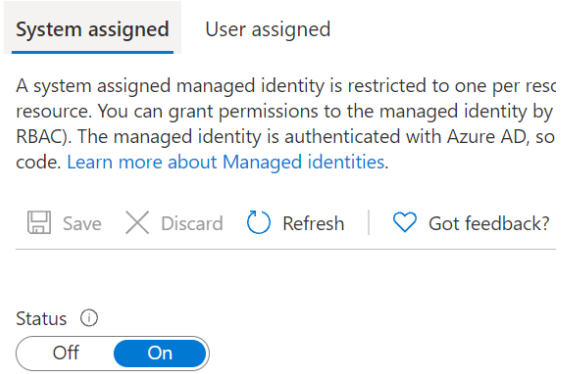
- Managed identity allows you to eliminate this part (dealing with creds)
- It is an **account** in **Azure Active Directory**
- Call the managed identity using **Connect-AzAccount -Identity**

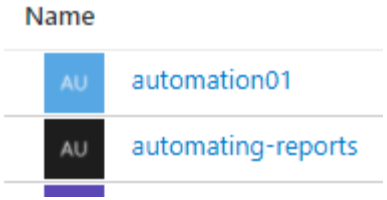
Here are some of the benefits of using managed identities:

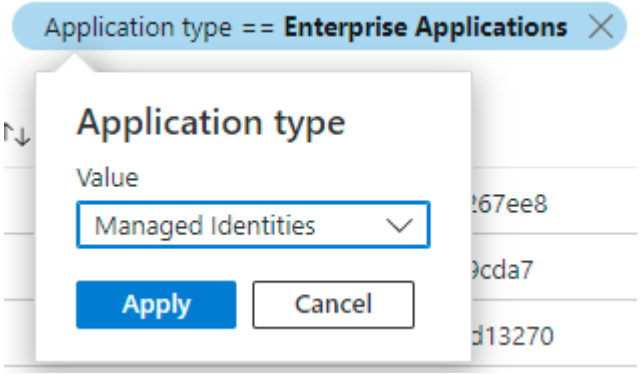
- You don't need to manage credentials. Credentials aren't even accessible to you.
- You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.
- Managed identities can be used without any additional cost.

Managed identities: how to implement it ?

1. Go to **Automation** > **Identities** > enable **System assigned**
2. This will create an Azure Enterprise application
3. Add permissions with PowerShell (can not be done through portal)
4. Call the managed identity with **Connect-AzAccount -Identity**







Demo: send custom data

What will we see ?

- Basic Remediation script
- Drivers inventory script
- Basic Azure Automation runbook
- Automation + Graph + Log Analytics

Demo: custom reporting

What will we see ?

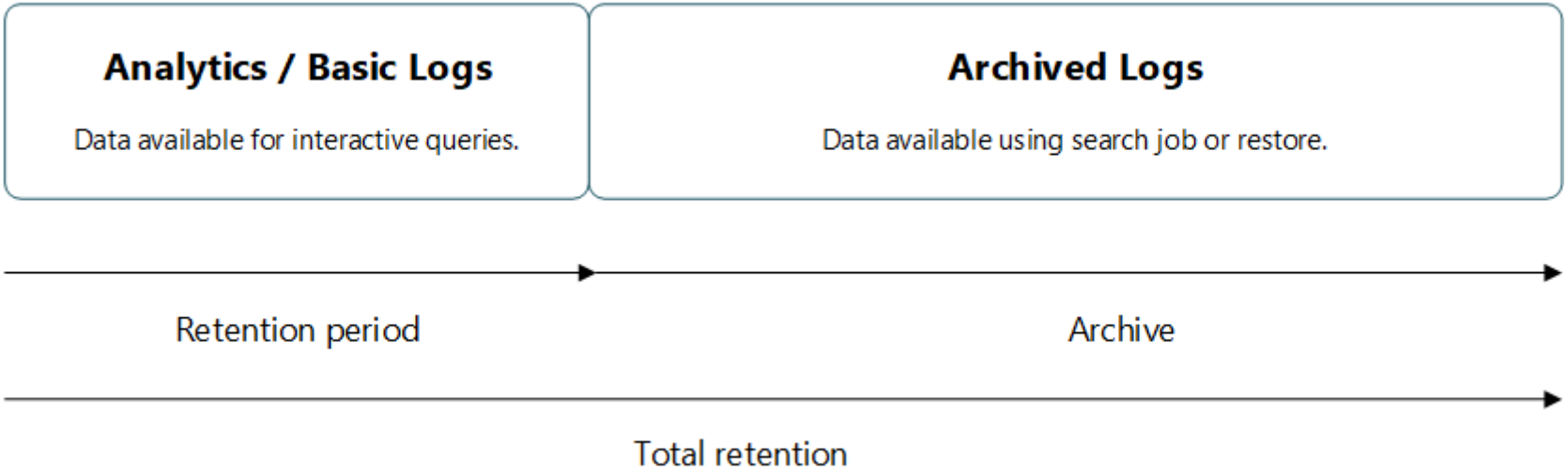
- Creating quick lab from CSV
- Creating a workbook in live

Going further

MODERN
ENDPOINT
MANAGEMENT
SUMMIT 2023

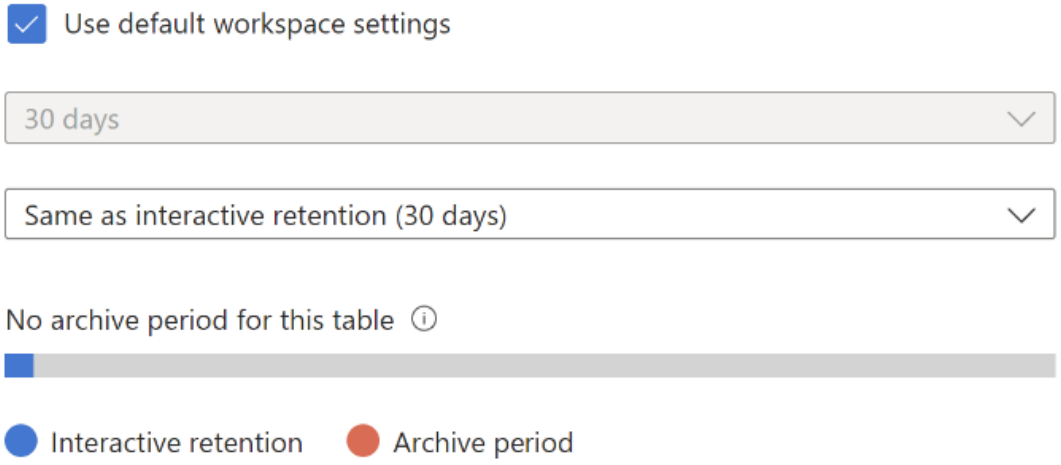
Data retention

- **Retention ?** When data will be removed/archived from your workspace
- Archiving allows you to keep older or less used data at a reduced cost



Data retention

- **<u>Default retention period is 30 days</u>**, but you can create a new policy
- You can customize data retention period by managing tables



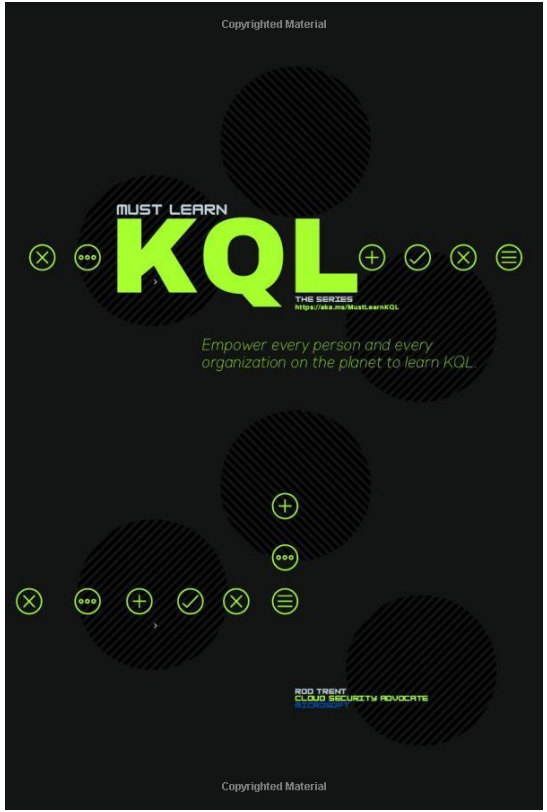
Log Analytics demo env

- https://aka.ms/LADemo
- Demo site provided by MS
- Can be used to learn the KQL at no cost to you

- Active Directory Health Check
- Azure Monitor for VMs
- AzureResources
- Change Tracking
- ContainerInsights
- LogManagement
- Microsoft Sentinel
- Network Performance Monitor
- Security and Audit
- SecurityCenterFree
- Service Map

KQL search

- Blog post series about KQL by Rod Trent
- https://github.com/rod-trent/MustLearnKQL
- Book available: https://a.co/d/fINFGnw

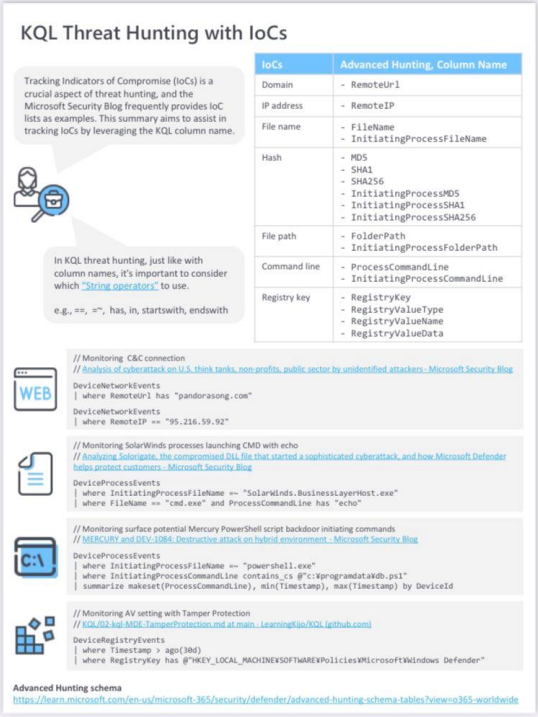


KQL threat hunting

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

Using KQL for threat hunting by Kijo Niimura

https://github.com/LearningKijo/KQL/blob/main/KQL-Effective-Use/10-kql-ThreatHunting-IoCs-tips-v1.pdf.pdf



KQL Threat Hunting with IoCs

Tracking Indicators of Compromise (IoCs) is a crucial aspect of threat hunting, and the Microsoft Security Blog frequently provides IoC lists as examples. This summary aims to assist in tracking IoCs by leveraging the KQL column name.

In KQL threat hunting, just like with column names, it's important to consider which "String operators" to use.

e.g., ==, =~, has, in, startswith, endswith

IoCs	Advanced Hunting, Column Name
Domain	- RemoteUrl
IP address	- RemoteIP
File name	- FileName - InitiatingProcessFileName
Hash	- MD5 - SHA1 - SHA256 - InitiatingProcessMD5 - InitiatingProcessSHA1 - InitiatingProcessSHA256
File path	- FolderPath - InitiatingProcessFolderPath
Command line	- ProcessCommandLine - InitiatingProcessCommandLine
Registry key	- RegistryKey - RegistryValueType - RegistryValueName - RegistryValueData

```
// Monitoring  C&C connection
// Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers - Microsoft Security Blog

DeviceNetworkEvents
| where RemoteUrl has "pandorasong.com"

DeviceNetworkEvents
| where RemoteIP == "95.216.59.92"
```

```
// Monitoring SolarWinds processes launching CMD with echo
// Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers - Microsoft Security Blog

DeviceProcessEvents
| where InitiatingProcessFileName =~ "SolarWinds.BusinessLayerHost.exe"
| where FileName == "cmd.exe" and ProcessCommandLine has "echo"
```

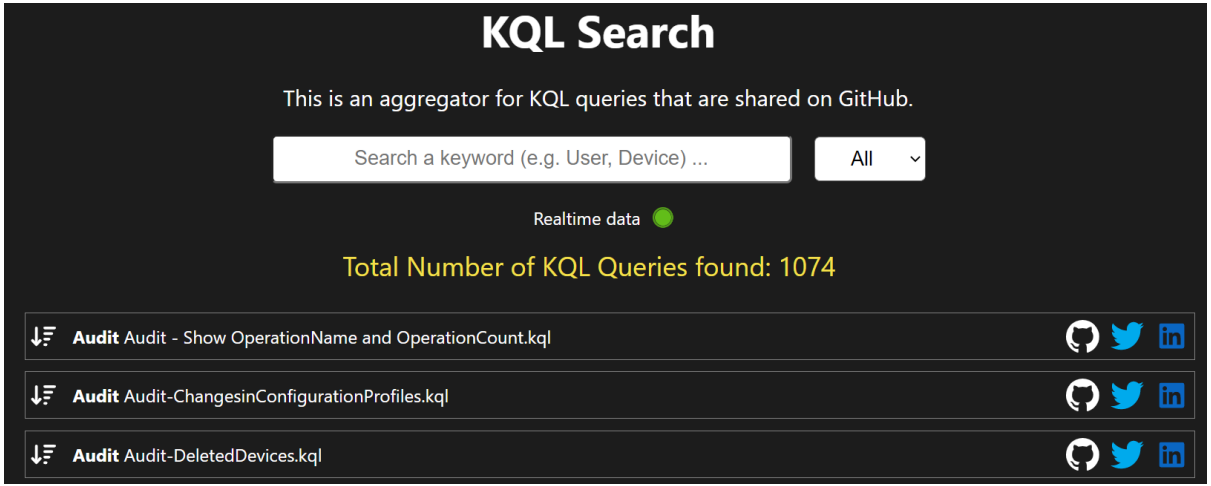
```
// Monitoring surface potential Mercury PowerShell script backdoor initiating commands
// MERCURY and DEV-1084: Destructive attack on hybrid environment - Microsoft Security Blog

DeviceProcessEvents
| where InitiatingProcessFileName =~ "powershell.exe"
| where InitiatingProcessCommandLine contains_cs @"c:¥programdata¥db.ps1"
| summarize makeset(ProcessCommandLine), min(Timestamp), max(Timestamp) by DeviceId
```

```
// Monitoring AV setting with Tamper Protection
// KQL/02-kql-MDE-TamperProtection.md at main · LearningKijo/KQL (github.com)

DeviceRegistryEvents
| where Timestamp > ago(30d)
| where RegistryKey has @"HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows Defender"
```

Advanced Hunting schema
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-schema-tables?view=o365-worldwide

KQL search

- Created by Ugur Koc (@UgurKocDe)
- https://www.kqlsearch.com



Thank you!!

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

SILVER SPONSOR

PATCH MY PC

Rimo3

METSYS

MODERN ENDPOINT MANAGEMENT SUMMIT 2023 EMEA EDITION

MODERN ENDPOINT MANAGEMENT SUMMIT 2023

GOLD SPONSOR

Microsoft

DELL Technologies

6th-7th september