



# MICROSOFT PURVIEW ADVANCED RICH REPORTS FOR POWER BI AND SENTINEL

BASED ON OFFICE 365 MANAGEMENT API, MICROSOFT GRAPH API, AIP SERVICE API AND OFFICE 365 EXCHANGE ONLINE API

(JANUARY 2023)



<https://aka.ms/MPARR-GitHub>

Sebastián Zamorano A.  
ISD Senior Consultant



# GRATITUDE

*My special gratitude to all my colleagues that helped and supported me on this new release. Special thanks to Grzegorz Berdzik, our black belt in this script; Dominik Kot who share some ideas and present me to Grzegorz; Stephan Carsten that who put some order in this script. And others that contact me constantly to ask for this, they make a lot of pression and now is here.*

*Additional thanks to Florian Boigner who is guide me on the Power BI path, as a good instructor.*

*We cannot forget to Walid Elmorsy who is the owner of the original script used for all of this.*

*Really thanks to all  
Sebastián Andrés Zamorano Andrade*



# AGENDA

WHAT WILL WE HAVE FOUND HERE?

## WHAT WILL WE HAVE FOUND HERE?

- **SAMPLES OF QUERIES AND REPORTS THAT CAN BE CREATED**
- **GENERAL CONCEPTS**
- **PREREQUISITES**
- **BASELINE CONFIGURATION**
- **POWER BI CONFIGURATION**
- **ADVANCED SETTINGS**



# DASHBOARDS

SOME SAMPLE REPORTS

## DASHBOARD FOR UNIFIED LABELING BEHAVIOR

### Unified Labeling

Overview

8

Number of files

6

Number of user owned files

5

Number of labeled files

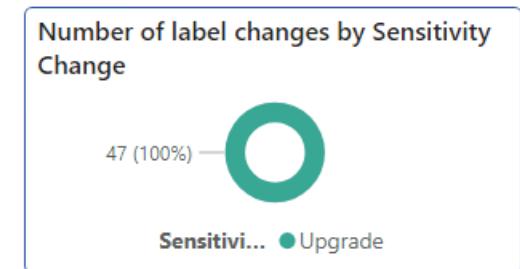
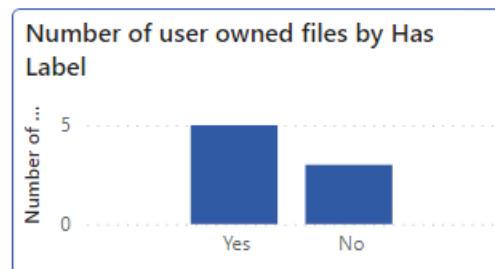
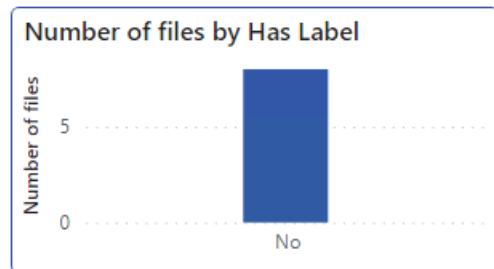
Filtering

Department

HR

Country\_s

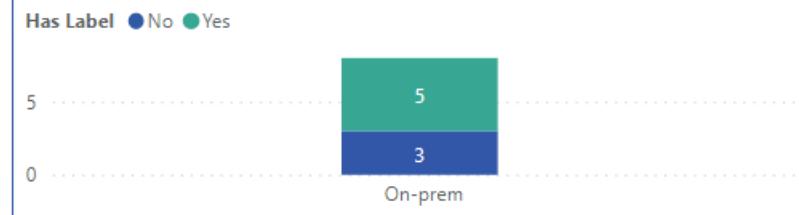
Poland



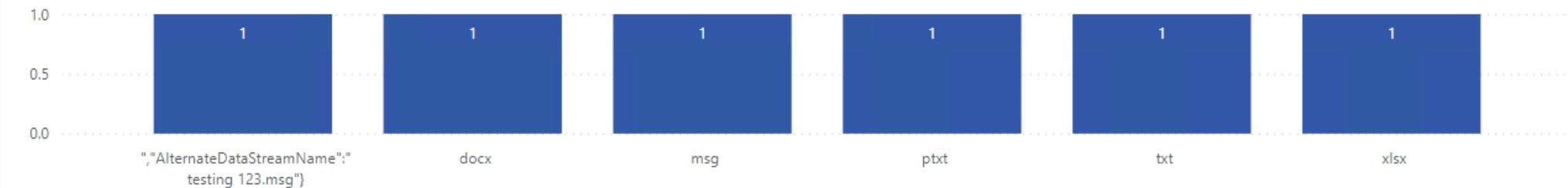
### Labeled files by label name



### Number of user owned files by WebService and Has Label



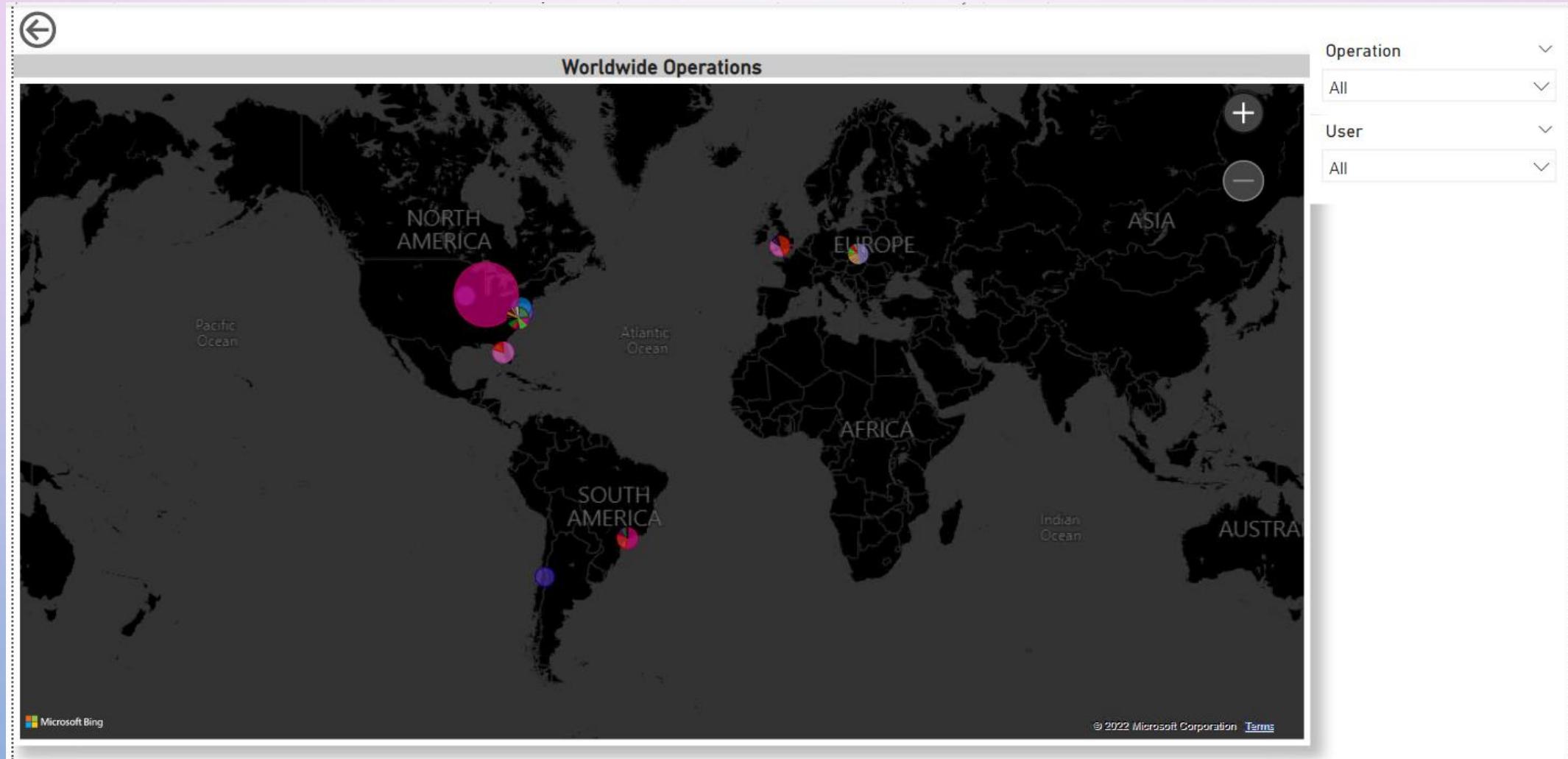
### File count by extension



Microsoft

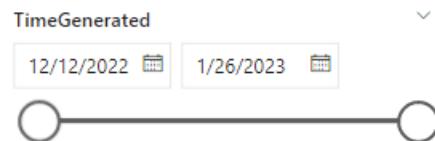
## DASHBOARD – GEO LOCATION

### DASHBOARD FOR AUDIT ACTIVITIES



# DASHBOARD – USER BEHAVIOR

## DASHBOARD FOR DLP ACTIVITIES



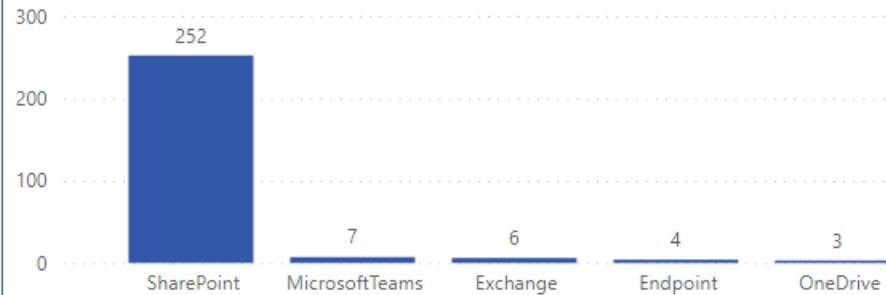
**272**

Number of DLP rule matches

### Number of DLP rule matches by Department\_s



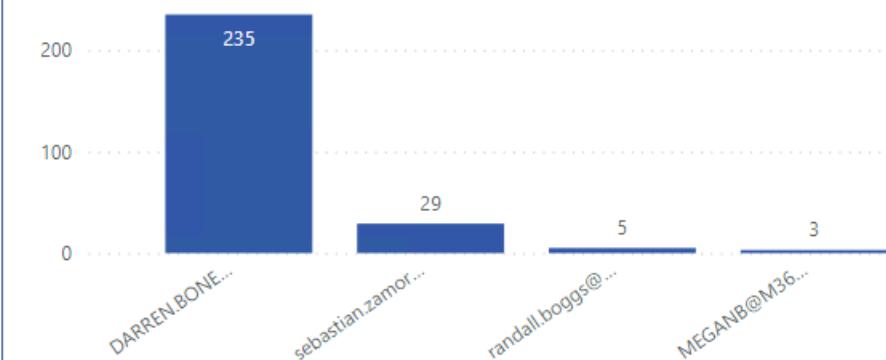
### DLP rule matches by workload



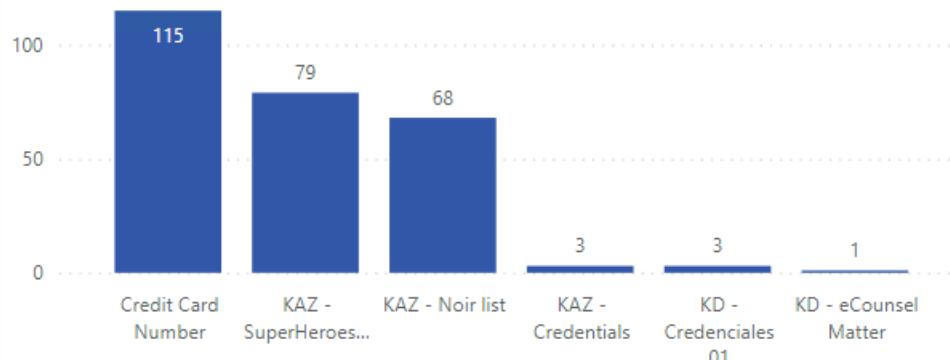
### DLP rule matches by date



### DLP rule matches by User



### DLP rule matches by SIT Detected



Right click on SIT Detected for drill-down to the details page

microsoft

# DASHBOARD – AIP SCANNER

## DASHBOARD FOR AUDIT ACTIVITIES

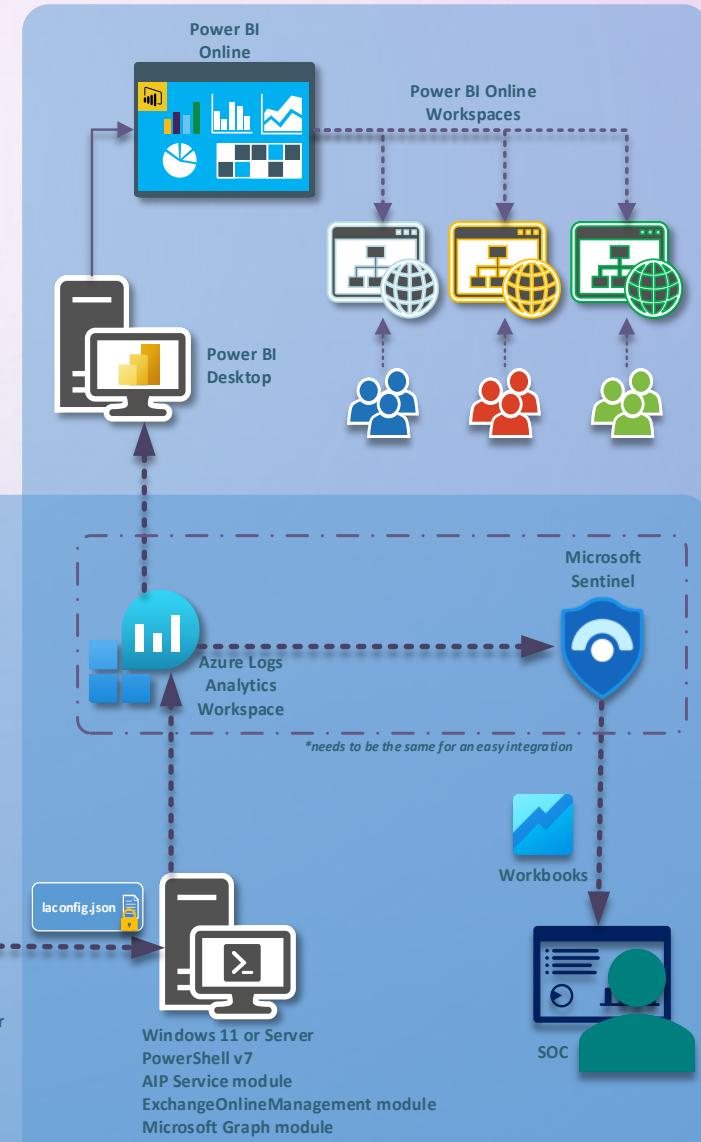
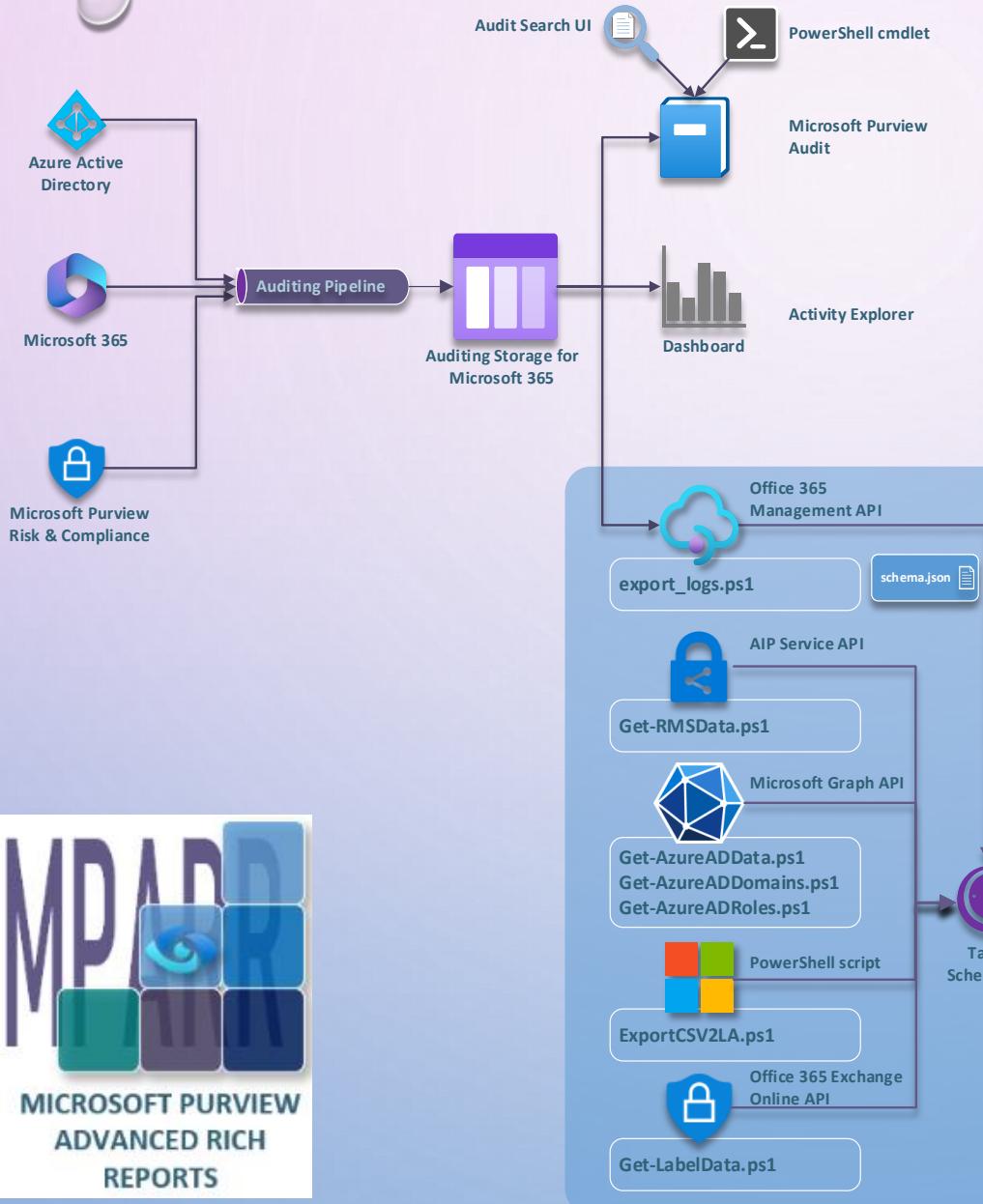


# SOME STUFFS TO TAKE ON MIND

The Information showed in the previously slides require do some steps to go from Kusto Query to Power BI, please find that information next



# GENERAL SOLUTION



Microsoft

# HAVE I ALL TO OBTAIN RESULTS?

**CERTS FOLDER:** TO EXECUTE THE **GET-XXXXX** SCRIPTS WE NEED SET SOME PERMISSIONS BASED ON CERTIFICATES, INSIDE OF THIS FOLDER YOU WILL FIND A **CREATECERTIFICATE.PS1** SCRIPT, USED FOR THAT FUNCTION.

**LOGS FOLDER:** HERE THE **TIMESTAMP.JSON** FILE IS SET (THIS FILE IS USED FOR **EXPORT\_LOGS.PS1** SCRIPT) AND ADDITIONAL ANY ERROR IS RECORD HERE (THE DEFAULT FOLDER IS LOCATED ON C:\APILOGS)

**SUPPORT FOLDER:** CONTAINS THE DOCUMENT USED TO CREATE THE TABLE WITH SERVICE PLAN AND FRIENDLY NAMES, THAT CAN BE DOWNLOADED FROM [HERE](#)

**LACONFIG.JSON:** THIS FILE CONTAINS THE KEYS AND DATA REQUIRE TO EXECUTE THE NEXT SCRIPTS; THE DATA RELATED TO KEYS CAN BE ENCRYPTED.

**SCHEMAS.JSON:** THIS FILE CONTAINS THE NAMES OF THE CONTENT BLOBS USED BY THE OFFICE 365 MANAGEMENT API, AND THE COLLECTOR TAKES THE INFORMATION FROM THESE ONES, IF SOME INFORMATION CANNOT BE COLLECTED, THE VALUE NEEDS TO BE CHANGE FROM TRUE TO FALSE.

**EXPORT\_LOGS.PS1:** SCRIPT USED TO OBTAIN THE DATA FROM OFFICE 365 MANAGEMENT API AND SEND TO LOGS ANALYTICS, TO USE WITH PARAMETERS THROUGH TASK SCHEDULER A NEW FILE NEEDS TO BE CREATED CALLED **RUN\_ME.PS1**

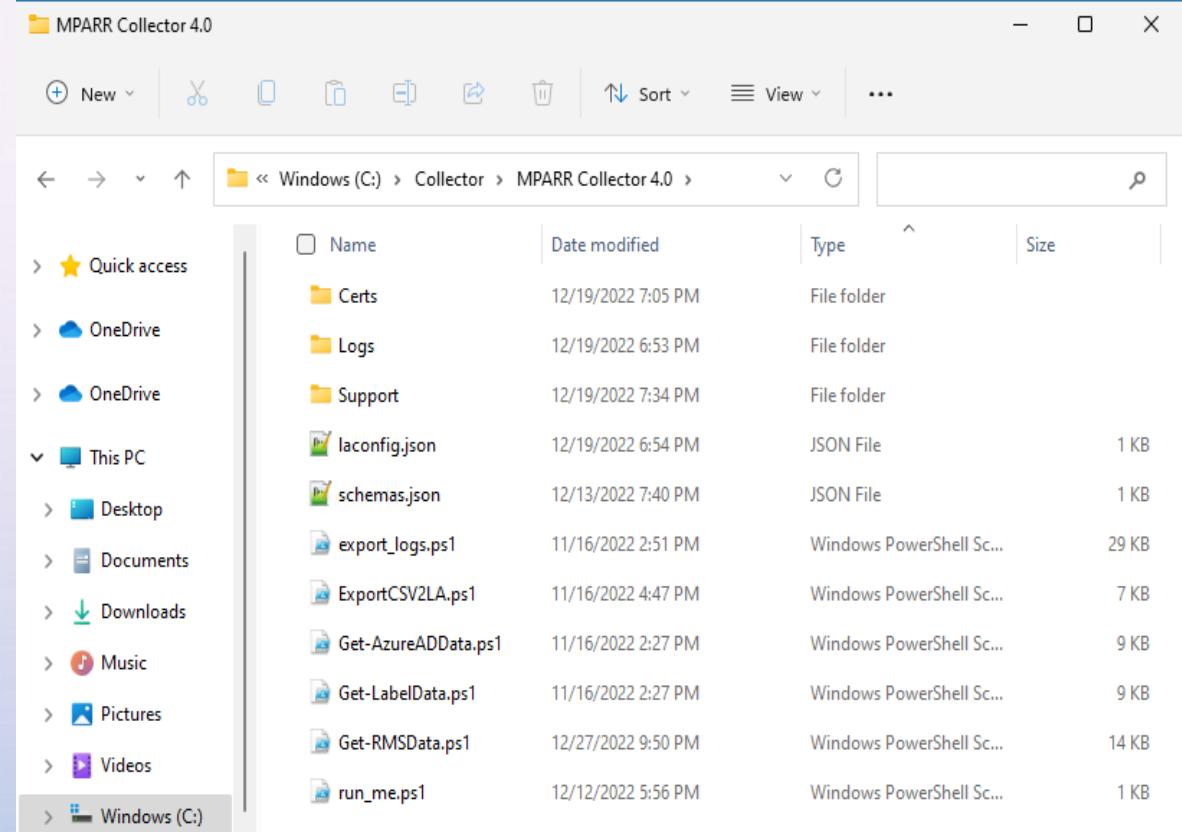
**EXPORTCSV2LA.PS1:** SCRIPT USED TO EXPORT THE CSV FILE (LOCATED ON SUPPORT FOLDER) WITH SERVICE PLAN TO LOGS ANALYTICS (REQUIRED TO EXECUTE ON-DEMAND)

**GET-AZUREADDATA.PS1:** SCRIPT USED TO COLLECT DATA FROM AZURE AD USING MICROSOFT GRAPH API, PERMISSIONS ARE ADDED TO AZURE AD APP FOR UNATTENDED EXECUTION, CAN BE MODIFIED TO ADD OR REMOVE CERTAIN AZURE AD ATTRIBUTES (CAN BE EXECUTE THROUGH TASK SCHEDULER MONTHLY, DEPENDING ON USERS' ROTATION)

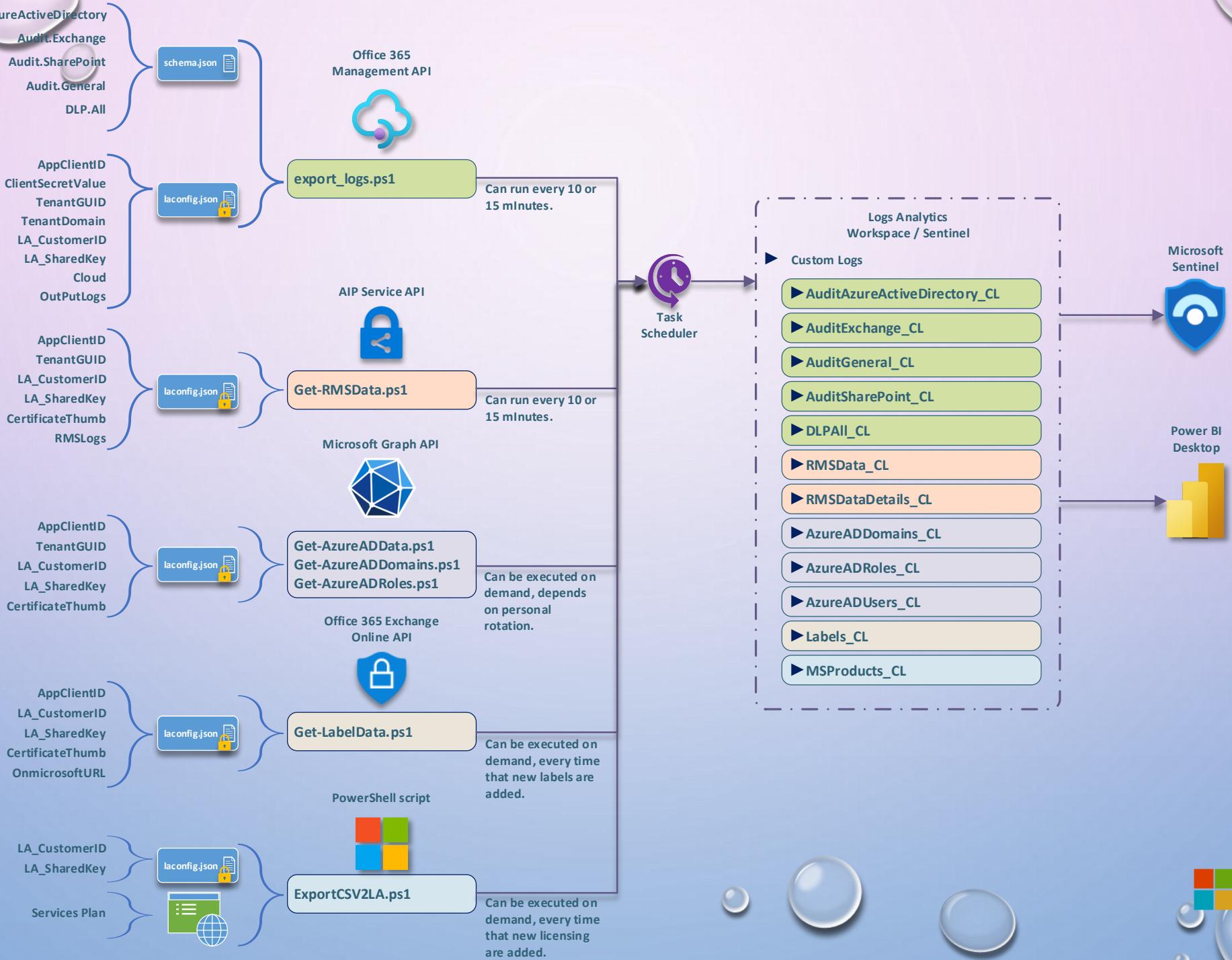
**GET-LABELDATA.PS1:** SCRIPT USED TO OBTAIN DISPLAY NAME AND ID FOR LABELS, REQUIRE EXCHANGEONLINEMANAGEMENT POWERSHELL MODULE, PERMISSIONS ARE ADDED TO AZURE AD APP FOR UNATTENDED EXECUTION (CAN BE EXECUTED ON-DEMAND)

**GET-RMSDATA.PS1:** SCRIPT USED TO OBTAIN INFORMATION ABOUT EXTERNAL ACCESS TO PROTECTED FILES, REQUIRE AIPSERVICE POWERSHELL MODULE, PERMISSIONS ARE ADDED TO AZURE AD APP FOR UNATTENDED EXECUTION , CAN BE EXECUTE WITH THE SAME TIMING AS **EXPORT\_LOGS.PS1**

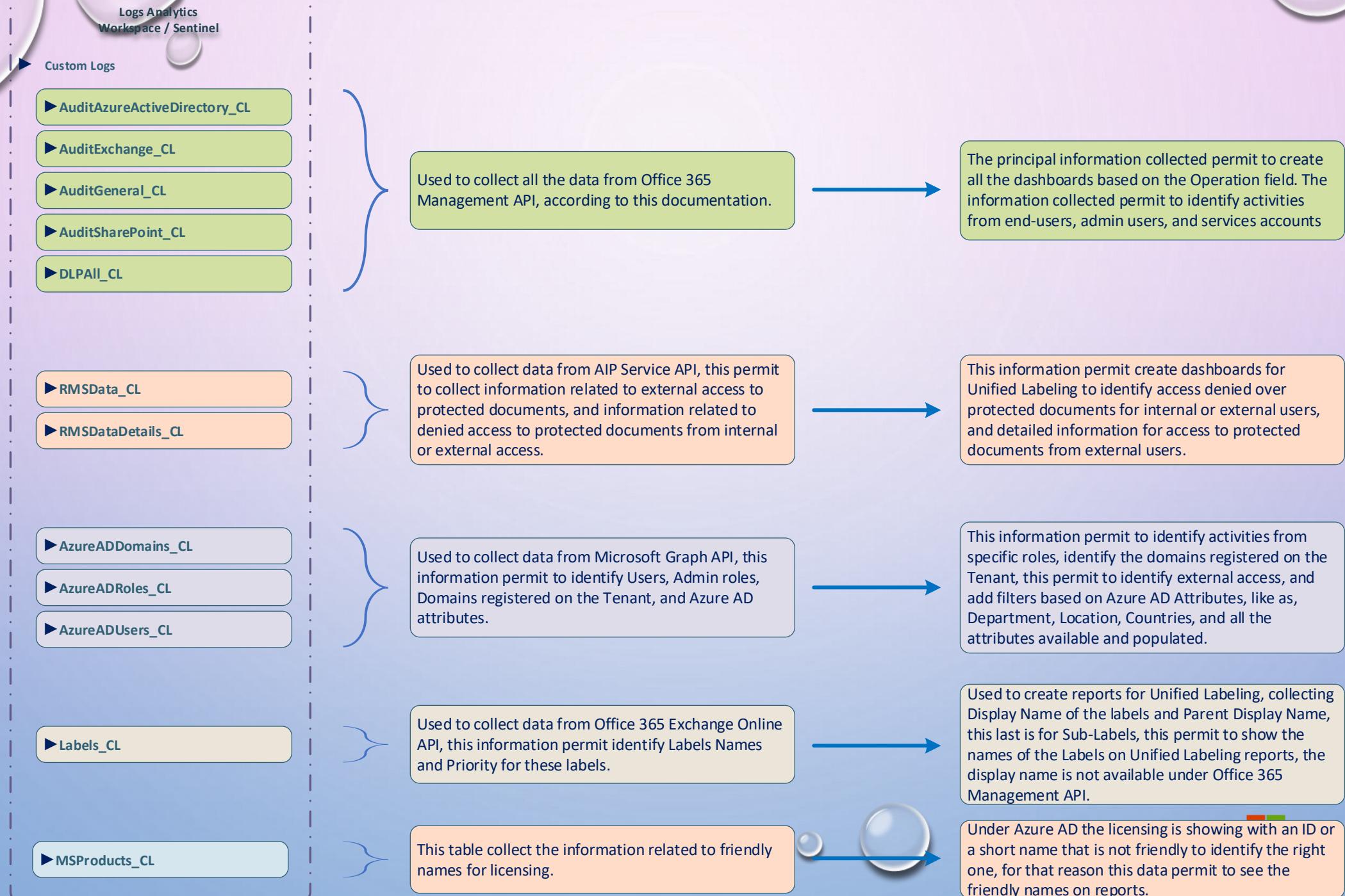
**RUN\_ME.PS1:** SCRIPT USED TO CALL **EXPORT\_LOGS.PS1** WITH PARAMETERS TO USE WITH TASK SCHEDULER



# DETAILED ARCHITECTURE



# DETAILED ARCHITECTURE



## PREREQUISITES TO IMPLEMENT

- LOGS ANALYTICS WORKSPACE (AZURE SUBSCRIPTION)
- WORKSTATION OR SERVER WITH INTERNET ACCESS
- POWERSHELL V7 INSTALLED ON THE PREVIOUS MACHINE
- EXCHANGEONLINEMANAGEMENT VERSION 3.0.0 MODULE FOR POWERSHELL
- MICROSOFT.GRAPH POWERSHELL MODULE INSTALLED
- AIPSERVICE MODULE FOR POWERSHELL
- AT LEAST APPLICATION ADMINISTRATOR TO CREATE AN APP UNDER AZURE AD
- COMPLIANCE ADMINISTRATOR ROLE TO OBTAIN SENSITIVITY LABELS LIST
- POWER BI DESKTOP
- OPEN URLs:
  - HTTPS://\*.AADRM.COM
  - HTTPS://\*.PROTECTION.OUTLOOK.COM
  - HTTPS://\*.AZURE.COM
  - HTTPS://MANAGE.OFFICE.COM (CAN BE DIFFERENT FOR GCC, GCCH OR DOD TENANTS)
  - HTTPS://GRAPH.MICROSOFT.COM
  - HTTPS://LOGIN.MICROSOFTONLINE.COM



## GO DIRECTLY FROM HERE TO THE SPECIFIC TOPICS

- AZURE AD APP CONFIGURATION →
- WORKSPACE LOGS ANALYTICS CONFIGURATION →
- CONFIGURE THE SCRIPT AND SET THE TASK SCHEDULER TASK →
- SELECT YOUR TENANT TYPE →
- GENERATE A CERTIFICATE TO EXECUTE SOME POWERSHELL CMDLETS UNATTENDED →
- CREATE A TABLE IN LOGS ANALYTICS WITH DISPLAY NAMES FOR LABELS AND IDS →
- GENERATE A TABLE IN LOGS ANALYTICS TO IDENTIFY LICENSING NAMES →
- ACCESS TO LOGS ANALYTICS AND EXPORT TO POWER BI CONSUME →
- CONFIGURE TO USE MICROSOFT GRAPH API THROUGH AZURE AD APP →
- GET USERS FROM AZURE AD WITH ATTRIBUTES AND LICENSING →
- CONNECT AND CONSUME THE DATA FROM POWER BI →
- CREATE AND CONSUME POWER BI TEMPLATES →
- GEO LOCATION ON POWER BI BASED ON IP ADDRESSES →

## CREATE APP TO RECOLLECT DATA (1/2)

- OPEN [HTTPS://PORTAL.AZURE.COM](https://portal.azure.com)
- LOOK FOR AZURE ACTIVE DIRECTORY
- GO TO “**APP REGISTRATIONS**” MENU
- PRESS **NEW REGISTRATION**
  - USE ANY NAME HERE
  - SELECT ACCOUNTS IN THIS ORGANIZATIONAL DIRECTORY ONLY
  - ON REDIRECT URI, SELECT WEB AND SET [HTTPS://LOCALHOST](https://localhost)
  - PRESS REGISTER
- ON THE NEW APP
  - COPY APPLICATION (CLIENT) ID AND DIRECTORY (TENANT) ID

### **TO GIVE UNATTENDED ACCESS**

- THEN GO TO CERTIFICATES & SECRETS, PRESS +NEW CLIENT SECRET AND SET A DESCRIPTION AND EXPIRATION TIME
- AFTER PRESS ADD BUTTON ON THE BLADE A NEW KEY WILL BE CREATED, COPY THAT KEY UNDER VALUE COLUMN
- UNDER CERTIFICATES TAB, ON THE SAME MENU, SELECT UPLOAD CERTIFICATE
- SELECT THE CERTIFICATE CREATED ON [THIS STEP](#) AND ADD A DESCRIPTION.

## CREATE APP TO RECOLLECT DATA (2/2)

- ON THE NEW APP (COMING FROM PREVIOUS PAGE)
  - GO TO API PERMISSIONS AND SELECT +ADD A PERMISSION:

### **TO GIVE ACCESS TO OFFICE 365 MANAGEMENT API**

- AT THE BLADE OPEN LOOKING FOR OFFICE 365 MANAGEMENT APIs
- AFTER SELECT THIS APPLICATION, CLICK ON APPLICATION PERMISSIONS
- SELECT THE 3 OPTIONS AVAILABLE, CHECK ALL OF THEM, AND THEN PRESS ADD PERMISSIONS BUTTON AT THE FINAL OF THAT BLADE

### **TO GIVE ACCESS TO MICROSOFT GRAPH**

- AT THE BLADE OPEN LOOKING FOR MICROSOFT GRAPH
- AFTER SELECT THIS APPLICATION, CLICK ON APPLICATION PERMISSIONS
- SELECT AUDITLOG.READ.ALL, DIRECTORY.READ.ALL, GROUP.READ.ALL, ORGANIZATION.READ.ALL, USER.READ.ALL

### **TO GIVE ACCESS TO COMPLIANCE POWERSHELL CONSOLE (ADDITIONAL PERMISSION IS REQUIRED [HERE](#))**

- AT THE BLADE OPEN LOOKING, AT TOP SELECT THE TAB “APIS MY ORGANIZATION USES”
- SEARCH FOR “OFFICE 365 EXCHANGE ONLINE”
- AFTER SELECT THIS APPLICATION, CLICK ON APPLICATION PERMISSIONS
- UNDER EXCHANGE SUBMENU SELECT “EXCHANGE.MANAGEASAPP”

### **TO GIVE ACCESS TO AIP SERVICE API (AZURE RIGHTS MANAGEMENT SERVICES)**

- AT THE BLADE OPEN LOOKING FOR AZURE RIGHTS MANAGEMENT SERVICES
  - AFTER SELECT THIS APPLICATION, CLICK ON APPLICATION PERMISSIONS
  - SELECT APPLICATION.READ.ALL
- PRESS “ADD PERMISSIONS” IN ALL THE CASES



# AZURE AD

## STEPS

The screenshot shows the Azure Active Directory (Azure AD) service page in the Azure portal. At the top, there's a search bar with the text "Azure acti". Below it, a navigation bar includes tabs for "All", "Services (92)", "Resources", "Resource Groups", "Marketplace", and "Documentation". A sub-menu for "Azure Active Directory" is open under the "Services" tab.

**Welcome to Azure Active Directory**

Don't have a subscription? [Get started with Azure free trial](#)

**Services**

- Azure Active Directory** (selected)
- Security
- Azure Cosmos DB
- Azure Database for MySQL servers

See all

- Activity log
- Azure Arc
- Azure Databricks
- Automanage – Azure machine best practices

[Give feedback](#)

**Start with an Azure free trial**

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

[Start](#) [Learn more](#)

**Manage Azure Active Directory**

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#) [Learn more](#)

**Access student benefits**

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more](#)

**Azure services**

[Create a resource](#)

**Azure Active Directory**

**Azure Information...**

**Microsoft Purview...**

**Azure AD B2C**

**Azure AD Privileged...**

**Help + support**

**Microsoft Sentinel**

**Function App**

[More services](#)

**Resources**

**Recent** **Favorite**

Name	Type	Last Viewed

No resources have been viewed recently

[View all resources](#)



## STEPS

The screenshot shows the Azure Active Directory (AAD) Overview page for the tenant 'Kaz Demos'. The left sidebar lists various management options like Users, Groups, External Identities, etc., with 'App registrations' highlighted. The main content area displays basic information about the tenant, including its name ('Kaz Demos'), tenant ID, primary domain ('kazdemos.org'), and license ('Azure AD Premium P2'). It also shows statistics for users (31), groups (59), applications (7), and devices (7). A warning message at the bottom right alerts about the deprecation of TLS 1.0, 1.1, and 3DES, encouraging users to enable support for TLS 1.2.

Home >

### Kaz Demos | Overview

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names

Add Manage tenants What's new Preview features Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

Overview Monitoring Properties Tutorials

Search your tenant

**Basic information**

Name	Kaz Demos	Users	31
Tenant ID	[REDACTED]	Groups	59
Primary domain	kazdemos.org	Applications	7
License	Azure AD Premium P2	Devices	7

**Alerts**

**Upcoming TLS 1.0, 1.1 and 3DES deprecation**

Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Learn more

# STEPS

Home > Kaz Demos | App registrations >

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Office 365 Management API capture ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Kaz Demos only - Single tenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▾ https://localhost ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) ↗

[Register](#)



## STEPS

Home > Kaz Demos | App registrations >

### Office 365 Management API capture

Search (Ctrl+ /) Delete Endpoints Preview features

Overview Quickstart Integration assistant

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

**Essentials**

Display name : [Office 365 Management API capture](#)  
Application (client) ID : 827e1a00-3000-459c-9104-2900cf18b4a  
Object ID : 59817ef1-3d21-44a4-a0dd-27b4b09bf57c  
Directory (tenant) ID : ac1a...e00-100-2122d24f062c  
Supported account types : [My organization only](#)

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will co...

**Get Started** Documentation

Build



# STEPS

Home > Kaz Demos | App registrations > Office 365 Management API capture

Office 365 Management API capture | Certificates & secrets

Search (Ctrl+ /) Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
No client secrets have been created for this application.			

Add a client secret

Description: Collector

Expires: 24 months

## STEPS

Home > Kaz Demos | App registrations > Office 365 Management API capture

### Office 365 Management API capture | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

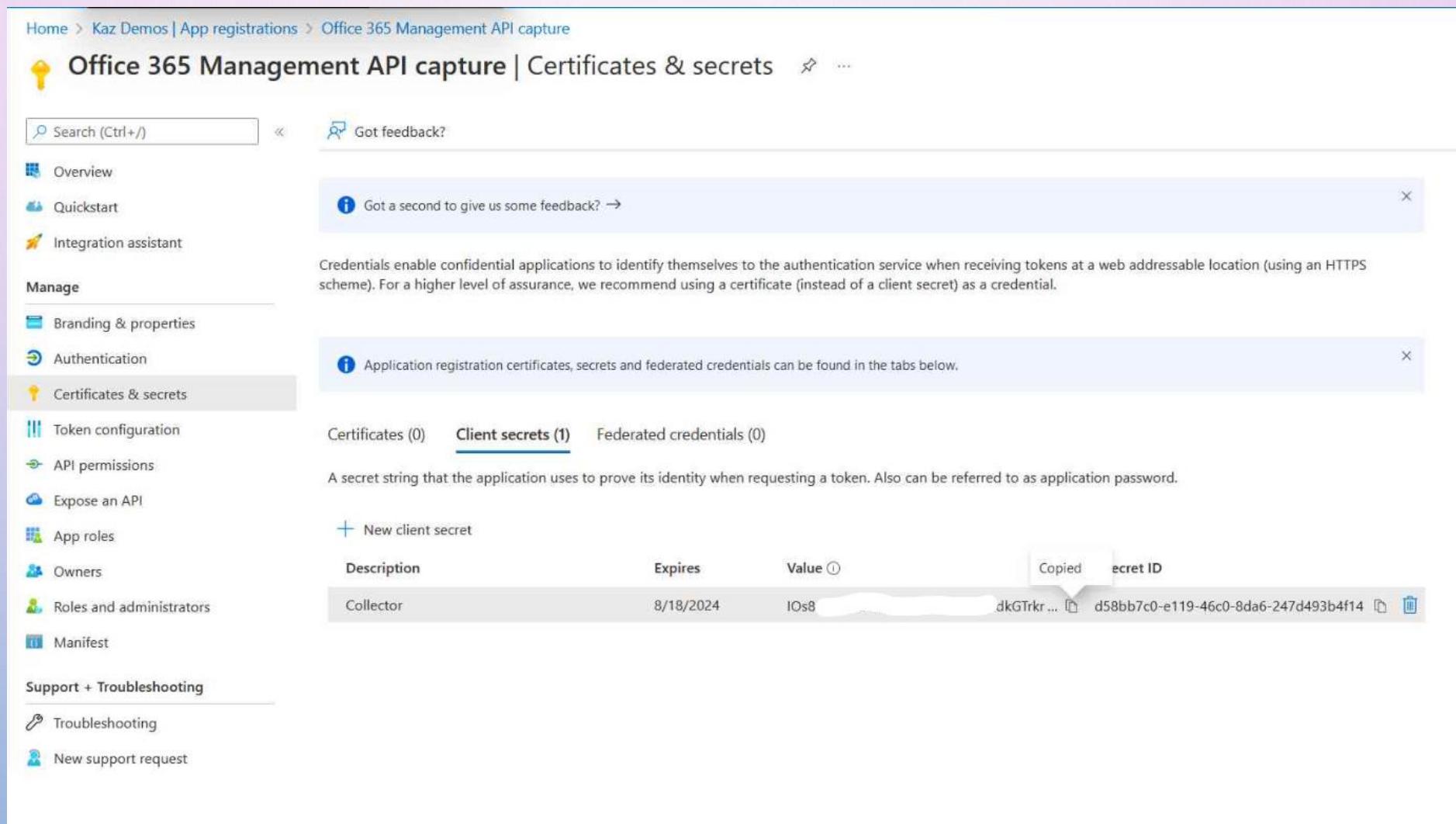
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value ⓘ	Copied	Secret ID
Collector	8/18/2024	IOs8	dkGTrkr ...	d58bb7c0-e119-46c0-8da6-247d493b4f14

Troubleshooting New support request



## STEPS

Home > Kaz Demos | App registrations > Microsoft Purview Reports

### Microsoft Purview Reports | Certificates & secrets

Search Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

**Certificates (1)** Client secrets (3) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
180	7917... Microsoft Purview	10/11/2022	10/11/2023	dc535e74-a958-4eea-...  



# STEPS

The screenshot shows two windows side-by-side. On the left is the 'Office 365 Management API capture | API permissions' page in the Azure portal. The URL is [https://manage.office.com/applications/KazDemos/apiPermissions](#). The page displays a table of configured permissions for the Microsoft Graph API. One permission is listed:

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)	User.Read	Delegated	Sign in and read user profile	No

The right window is a 'Request API permissions' modal for the 'Office 365 Management APIs'. It shows two options: 'Delegated permissions' (selected) and 'Application permissions'. The 'Delegated permissions' section notes that the application needs to access the API as the signed-in user.



## STEPS

### Request API permissions

[All APIs](#)



Office 365 Management APIs

<https://manage.office.com/> [Docs](#)

What type of permissions does your application require?

#### Delegated permissions

Your application needs to access the API as the signed-in user.

#### Application permissions

Your application runs as a background service or daemon without a signed-in user.

#### Select permissions

[expand all](#)



Start typing a permission to filter these results

##### Permission

##### Admin consent required

##### ActivityFeed (2)



ActivityFeed.Read ⓘ

Read activity data for your organization

Yes



ActivityFeed.ReadDlp ⓘ

Read DLP policy events including detected sensitive data

Yes

##### ServiceHealth (1)



ServiceHealth.Read ⓘ

Read service health information for your organization

Yes



## STEPS

**Request API permissions**

 Microsoft Graph  
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Start typing a permission to filter these results

Permission	Admin consent required
> AccessReview	
> Acronym	
> AdministrativeUnit	
> AgreementAcceptance	
> Agreement	
> APIConnectors	
> AppCatalog	
> Application	
> AppRoleAssignment	
> ...	

## STEPS

## Request API permissions

< All APIs

Office 365 Exchange Online  
https://ps.outlook.com

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Start typing a permission to filter these results

Permission	Admin consent required
full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	
Exchange (1)	
Exchange.ManageAsApp ⓘ Manage Exchange As Application	Yes
IMAP	
Mailbox	

## STEPS

## Request API permissions

[All APIs](#)

Azure Rights Management Services  
<https://aadrm.com/> [Docs](#)

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
<input checked="" type="checkbox"/> Application.Read.All ⓘ Read all service configuration and log data for the Azure Information Protection service.	Yes
<b>Content</b>	
<input type="checkbox"/> Content.DelegatedReader ⓘ Read protected content on behalf of a user	Yes
<input type="checkbox"/> Content.DelegatedWriter ⓘ Create protected content on behalf of a user	Yes
<input type="checkbox"/> Content.SuperUser ⓘ Read all protected content for this tenant	Yes
<input type="checkbox"/> Content.Writer ⓘ Create protected content	Yes

# STEPS

Home > Kaz Demos | App registrations > Microsoft Purview Reports

## Microsoft Purview Reports | API permissions

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Kaz Demos? This will update any existing admin consent records this application already has to match what is listed below.

Yes  No

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Rights Management Services				
Application.Read.All	Application	Read all service configuration and log data for the Azure I...	Yes	<span>Granted for Kaz Demos</span> ...
Microsoft Graph (6)				
AuditLog.Read.All	Application	Read all audit log data	Yes	<span>Granted for Kaz Demos</span> ...
Directory.Read.All	Application	Read directory data	Yes	<span>Granted for Kaz Demos</span> ...
Group.Read.All	Application	Read all groups	Yes	<span>Granted for Kaz Demos</span> ...
Organization.Read.All	Application	Read organization information	Yes	<span>Granted for Kaz Demos</span> ...
User.Read	Delegated	Sign in and read user profile	No	<span>Granted for Kaz Demos</span> ...
User.Read.All	Application	Read all users' full profiles	Yes	<span>Granted for Kaz Demos</span> ...
Office 365 Exchange Online (1)				
Exchange.ManageAsApp	Application	Manage Exchange As Application	Yes	<span>Granted for Kaz Demos</span> ...
Office 365 Management APIs (3)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	<span>Granted for Kaz Demos</span> ...
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	<span>Granted for Kaz Demos</span> ...
ServiceHealth.Read	Application	Read service health information for your organization	Yes	<span>Granted for Kaz Demos</span> ...

## CREATE A WORKSPACE IN LOGS ANALYTICS

- OPEN [HTTPS://PORTAL.AZURE.COM](https://portal.azure.com)
- LOOK FOR LOG ANALYTICS WORKSPACES
- PRESS +CREATE
  - SELECT YOUR AZURE SUBSCRIPTION
  - SELECT OR CREATE A RESOURCE GROUP
  - SET A NAME RELATED TO THIS WORKSPACE
  - SELECT THE REGION THAT BEST MATCH
  - PRESS REVIEW + CREATE, WAIT UNTIL A RESUME IS SHOW
  - PRESS CREATE
- WAIT UNTIL THE WORKSPACE BE SUCCESS DEPLOYED
- OPEN THE NEW WORKSPACE
- GO TO AGENTS MANAGEMENT MENU, AND OPEN LOG ANALYTICS AGENT INSTRUCTIONS
  - COPY WORKSPACE ID
  - COPY PRIMARY KEY

TO INTEGRATE WITH SENTINEL THE SAME LOGS ANALYTICS WORKSPACE IS NEEDED TO USE.



## STEPS

The screenshot shows the Azure portal search results for 'log Analytics'. The search bar at the top contains the query 'log Analytics'. Below the search bar, there are several filter buttons: All (selected), Services (17), Marketplace (7), Documentation (20), Resources (0), and Resource Groups (0). The 'Services' section is expanded, showing a list of services. The 'Log Analytics workspaces' item is highlighted with a gray background. Other services listed include Log Analytics query packs, Stream Analytics jobs, Data Lake Analytics, Azure Synapse Analytics, and Azure Synapse Analytics (private link hubs). The 'Marketplace' section lists Log Analytics Workspace, Logz.io - Cloud Monitoring and Observability, Cloud-Native Observability with Logz.io (LEGACY), and SEEPATH-managed-azure. The 'Documentation' section links to 'Overview of Log Analytics in Azure Monitor - Azure Monitor' and 'Create Log Analytics workspaces - Azure Monitor | Microsoft Docs'.

## STEPS

The screenshot shows the Microsoft Azure (Preview) interface for Log Analytics workspaces. The top navigation bar includes the Microsoft Azure logo, a search bar, and a refresh icon. Below the header, the breadcrumb navigation shows 'Home > Log Analytics workspaces'. The main title is 'Log Analytics workspaces' with a gear icon and three dots for more options. The URL is 'Microsoft (microsoft.onmicrosoft.com)'. The toolbar contains buttons for '+ Create', 'Open recycle bin', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. There are also filter buttons for 'Subscription equals 3 of 48 selected', 'Resource group equals all', 'Location equals all', and an 'Add filter' button. At the bottom, there are sorting options for 'Name' (with an up-down arrow), 'Resource group' (with an up-down arrow), and 'Location' (with an up-down arrow).

## STEPS

Home > Log Analytics workspaces >

## Create Log Analytics workspace

Basics Tags Review + Create

**i** 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 Internal Consumption (Preview) ...

Resource group \* ⓘ kazdemos.org Create new

**Instance details**

Name \* ⓘ M365Reports ✓

Region \* ⓘ Central US

Review + Create << Previous Next : Tags >

## STEPS

The screenshot shows the Microsoft Azure (Preview) interface with the title "Microsoft.LogAnalyticsOMS | Overview". The left sidebar includes "Home", "Deployment", "Overview" (which is selected), "Inputs", "Outputs", and "Template". The main content area displays a success message: "Your deployment is complete". It provides deployment details: Deployment name: Microsoft.LogAnalyticsOMS, Subscription: Microsoft Azure Internal Consumption (8c9c38d5-57e...), Resource group: kazdemos.org, Start time: 19/8/2022, 16:59:35, Correlation ID: fe71f61b-0d3f-4eeb-8ce6-3615b0384a1f. Below this, there are sections for "Deployment details" and "Next steps" with a "Go to resource" button.

## STEPS

The screenshot shows the Microsoft Azure (Preview) interface for the Log Analytics workspace 'M365Reports'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Agents management selected), Legacy agents management, Custom logs, Computer Groups, Data Export, Linked storage accounts, Network Isolation, Tables (preview), General (Workspace summary, Workbooks), and Metrics.

The main content area displays 'Windows servers' agent management. It shows 0 Windows computers connected via Azure Monitor Windows agent and 0 Windows computers connected via Log Analytics Windows agent (legacy). A button 'Data Collection Rules' is available for setting up the new Azure Monitor agent. Below this, under 'Log Analytics agent instructions', there is a section for 'Download agent' with links for Download Windows Agent (64 bit) and Download Windows Agent (32 bit). The 'Log Analytics Gateway' section provides instructions for machines with no internet connectivity.

Key workspace details shown in the UI:

- Workspace ID: 5703c95e-dec2-4c21-809b-d23d31c4c3c6
- Primary key: r5Bt8HlskQroE8zuhXaMh7GZvcheWPuDWKZ5On+NI9Tlv...
- Secondary key: T7yhxt/T2td0JBU9sn6hLNW8jwvCNZxLkE5jdkuz4jREa7TA...

A 'Regenerate' button is present next to each key.

## EXTEND YOUR DATA RETENTION UNTIL 2 YEARS

- UNDER GENERAL SELECT USAGE AND ESTIMATED COSTS AND THEN DATA RETENTION, SET DATA RETENTION PERIOD.

**MCAR-Kazdemos | Usage and estimated costs**

Log Analytics workspace

Search (Ctrl+ /) Usage details 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 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.

**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. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about Log Analytics pricing.

**Estimated costs**

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	2,76 US\$	0,00 GB	0,00 US\$
Microsoft Defender allowance	0,00 US\$	0,00 GB	0,00 US\$
Log data retention (beyond 31 days)	0,12 US\$	0,00 GB	0,00 US\$
<b>Total</b>			<b>0,00 US\$</b>

This is the current pricing tier.

**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) 730

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.

**Usage Charts**

Billable data ingestion per solution (I)

Date	Billable data ingestion (kB)
18 ago	~600
12	~350
19	~350

OK

Data ingested per solution (last 90 d: Category No data

## GENERATE A CERTIFICATE TO EXECUTE SOME POWERSHELL CMDLETS UNATTENDED

- WE WILL NEED TO **CREATE A CERTIFICATE** TO CONNECT TO INFORMATION PROTECTION SERVICES THROUGH AZURE AD APPLICATION, TO DO THAT THE 1<sup>ST</sup> STEP IS CREATE THAT CERTIFICATE:

- OPEN AN ISE POWERSHELL CONSOLE AND EXECUTE (SELECT A FOLDER 1<sup>ST</sup> TO SAVE THE 2 FILES CREATED, EXAMPLE C:\TMP):

```
# CREATE CERTIFICATE  
  
$MYCERT = NEW-SELFSGNEDCERTIFICATE -DNSNAME "KAZDEMONS.ORG" -CERTSTORELOCATION  
"CERT:\CURRENTUSER\MY" -NOTAFTER (GET-DATE).ADDYEARS(1) -KEYSPEC KEYEXCHANGE  
  
# EXPORT CERTIFICATE TO .PFX FILE  
  
$MYCERT | EXPORT-PFXCERTIFICATE -FILEPATH MYCERT.PFX -PASSWORD (GET-  
CREDENTIAL).PASSWORD  
  
# EXPORT CERTIFICATE TO .CER FILE  
  
$MYCERT | EXPORT-CERTIFICATE -FILEPATH MYCERT.CER
```

- ON THE 2ND LINE A PASSWORD WILL BE REQUIRED FOR PFX FILE, POWERSHELL WILL ASK FOR USER AND PASSWORD, BUT FINALLY ONLY PASSWORD WILL BE USED (ADD BOTH)
  - WE NEED TO USE THE SAME AZURE AD APPLICATION EXPLAINED [HERE](#)
  - UNDER THE SAME AZURE AD APP WE NEED GO TO “CERTIFICATES & SECRETS” MENU AND SELECT CERTIFICATES, THEN PRESS “UPLOAD CERTIFICATE” HERE IS REQUIRED THE FILE .CER, A NEW BLADE APPEAR, SELECT THE FOLDER ICON TO LOOKING FOR THE FILE AND OPEN THE FILE.
  - AFTER ADD COPY THE THUMBPRINT VALUE, WE WILL NEED TO ADD TO THE LACONFIG.JSON FILE
- A SCRIPT TO CREATE THE CERTIFICATE IS ADDED WITH THE REST OF THE SCRIPTS UNDER THE CERTS FOLDER, AND CALLED CREATECERTIFICATE.PS1, THIS SCRIPT CONTAINS THE SAME PREVIOUS CMDLETS.**



# CERTIFICATES CREATION

## STEPS

The screenshot shows a Windows PowerShell ISE window with two tabs: Untitled1.ps1\*(Recovered) and Untitled2.ps1\*(Recovered). The Untitled1.ps1 tab contains the following PowerShell script:

```
1 # Create certificate
2 $mycert = New-SelfSignedCertificate -DnsName "kazdemos.org" -CertStoreLocation "cert:\CurrentUser\My" -NotAfter (Get-Date).AddYears(1)
3
4 # Export certificate to .pfx file
5 $mycert | Export-PfxCertificate -FilePath KazDemosCertificate.pfx -Password (Get-Credential).password
6
7 # Export certificate to .cer file
8 $mycert | Export-Certificate -FilePath KazDemosCert
```

A credential dialog box titled "cmdlet Get-Credential at command pipeline position 1" is overlaid on the window. It asks for a User name (set to "NoMatter") and a Password (represented by a series of dots). The "OK" button is highlighted.

At the bottom of the PowerShell window, a status bar displays: "Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger." and "Ln 11 Col 1".



## STEPS

Home > Kaz Demos | App registrations > Microsoft Purview Reports

## Microsoft Purview Reports | Certificates & secrets

Search Got feedback?

Overview

Quickstart

Integration assistant

### Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Application registration certificates, secrets and federated credentials can be found in the tabs below.

**Certificates (1)** Client secrets (1) Federated credentials (0)

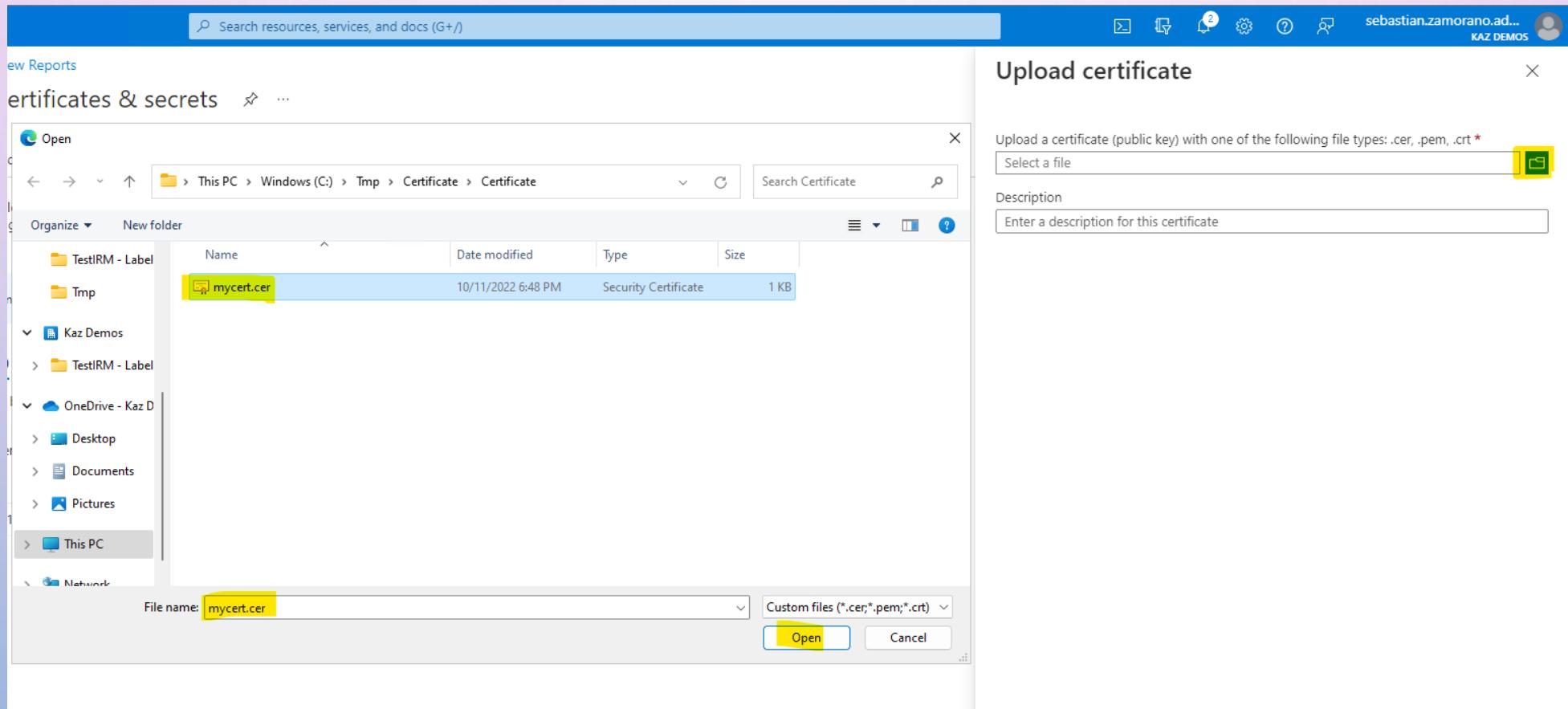
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
1808C721701BE04644F3D9FD107917...	Microsoft Purview	10/11/2022	10/11/2023	dc535e74-a958-4eea-... 



## STEPS



## STEPS

Certificates (1) Client secrets (1) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

↑ Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
1808C721701BE04644F3D9FD107917...	Microsoft Purview	10/11/2022	10/11/2023	dc535e74-a958-4eea-...

```
new 1 x new 2 x my_kazdemos_labels.csv x new 3 x new 4 x run_me.ps1 x new 5 x Get-auditLogs.ps1 x export_logs.ps1 x Get-LabelData.ps1 x laconfig.json x ExportCSV2LA.ps1 x
1 {
2     "EncryptedKeys": "True",
3     "AppClientID": "701a112f-2500-429f-8e13-aa51ca5af20",
4     "ClientSecretValue": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e30000000",
5     "TenantGUID": "a01a113-100e-4ac8-a4c9-52c",
6     "TenantDomain": "kazdemos.org",
7     "LA_CustomerID": "buzo511/-1a38-400j-adaf-a00,000,01-3",
8     "LA_SharedKey": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e30000000002",
9     "CertificateThumb": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e300000000",
10    "OnmicrosoftURL": "MC...36.onmicrosoft.com"
11 }
12 }
```

In this case the certificate thumbprint was encrypted using the steps explained in this [slide](#)

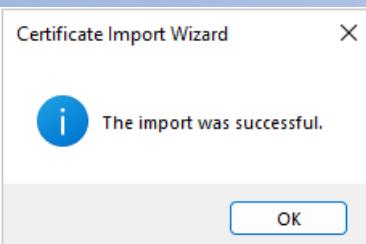
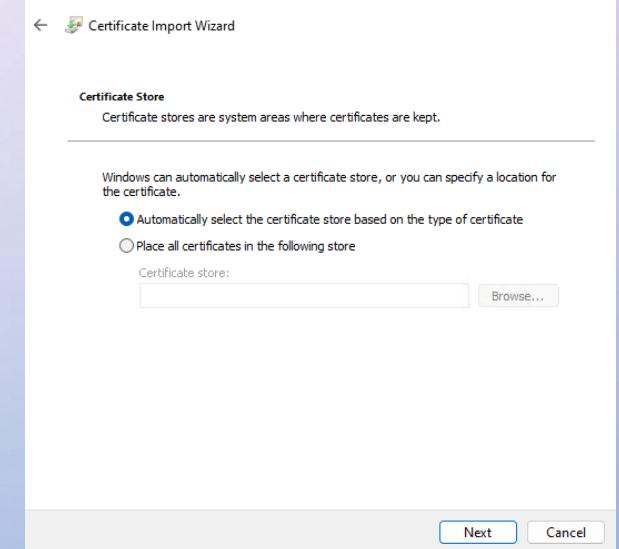
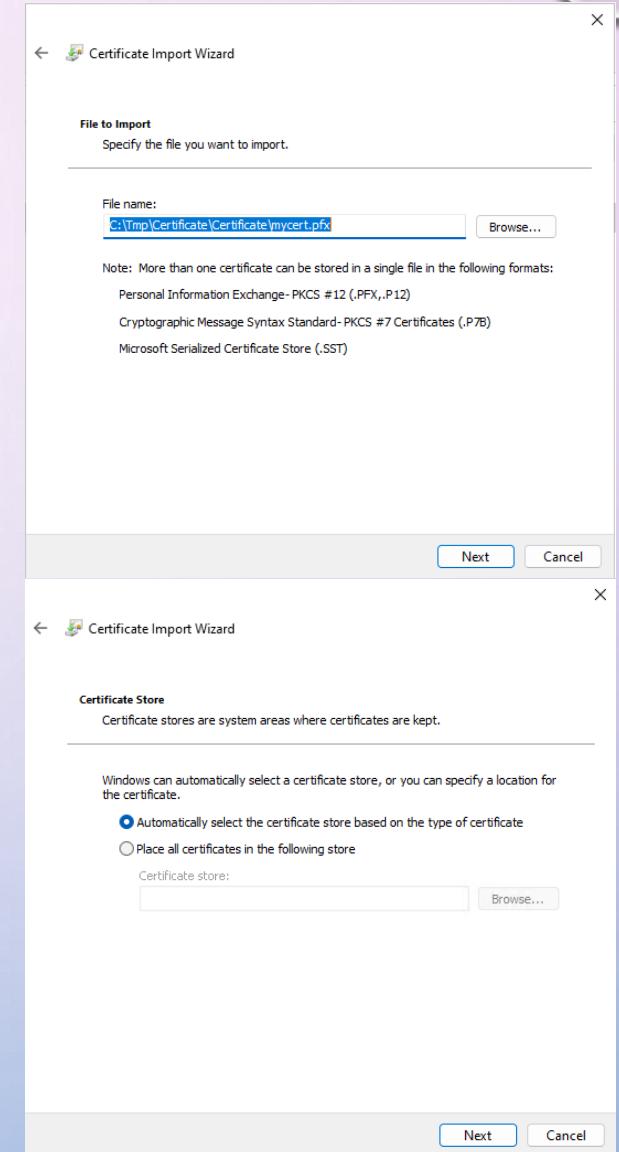
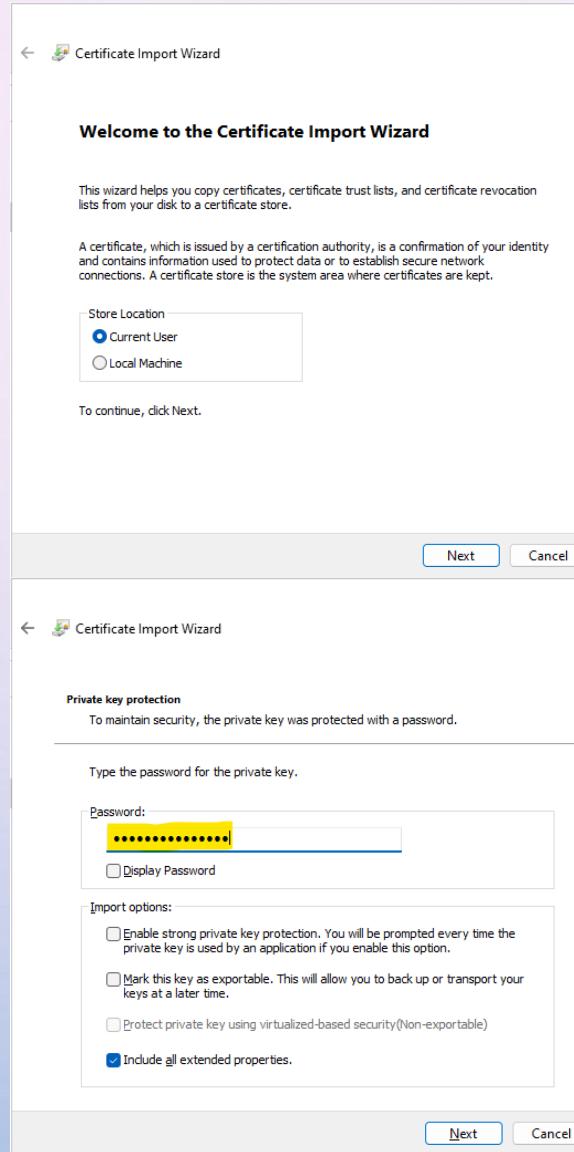
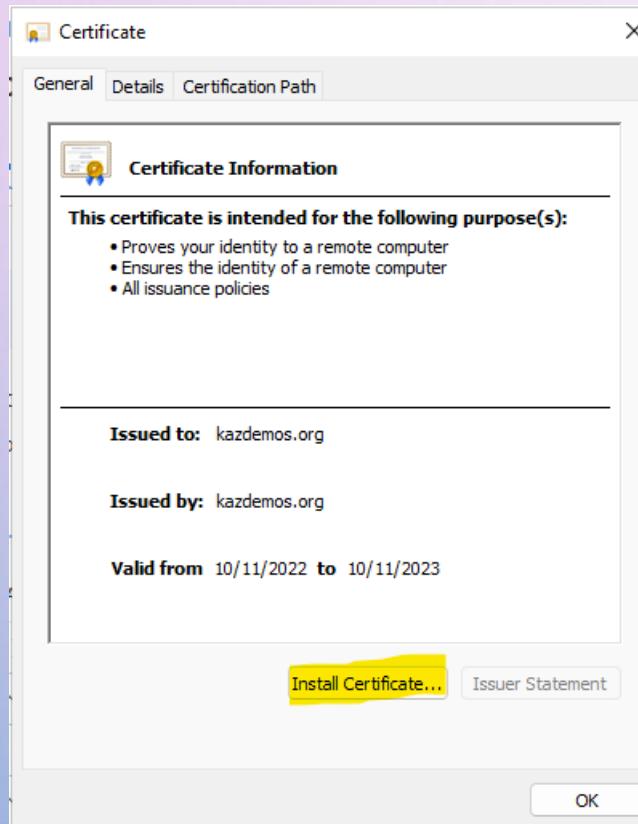


## TO EXECUTE THE SCRIPT USING THE CERTIFICATE

- ON THE SAME COMPUTER USED TO EXECUTE THE SCRIPTS IS NEEDED TO INSTALL BOTH CERTIFICATES PREVIOUSLY CREATED
- THE CERTIFICATES NEEDS TO BE INSTALLED ON THE SAME ACCOUNT USED TO EXECUTE THESE SCRIPTS:
  - GET-AZUREADDATA.PS1
  - GET-AZUREADDOMAINS.PS1
  - GET-AZUREADROLES.PS1
  - GET-LABELDATA.PS1
  - GET-RMSDATA.PS1(THIS ONE CAN BE EXECUTED ONLY USING POWERSHELL 5)
- TO INSTALL, IS REQUIRED PUT BOTH CERTIFICATES ON THE MACHINE USED TO EXECUTE THE SCRIPTS AND EXECUTE BOTH DOING DOUBLE CLICK.
- FOR EACH ONE IS REQUIRED TO INSTALL THE CERTIFICATE LOCALLY.

# INSTALL CERTIFICATE LOCALLY

## STEPS



Microsoft

## COMPLIANCE ADMINISTRATOR ROLE ASSIGNED TO AZURE AD APP

- TO EXECUTE GET-LABELDATA.PS1 SCRIPT ADDITIONAL PERMISSIONS ARE REQUIRED:
  - TO GIVE THE PERMISSIONS IS REQUIRED OPEN AZURE ACTIVE DIRECTORY
  - THEN GO TO “ROLES AND ADMINISTRATORS” MENU
  - SEARCH FOR COMPLIANCE ADMINISTRATOR AND PRESS THE NAME
  - IN THE NEW WINDOW CLICK OVER “+ ADD ASSIGNMENTS”
  - UNDER ADD ASSIGNMENTS INTERFACE, PRESS UNDER “SELECT MEMBER(S)” AND LOOKING FOR THE NAME OF THE AZURE AD APP PREVIOUSLY CREATED, CLICK IT OVER THE NAME AND PRESS SELECT
  - PRESS THE NEXT BUTTON, AND IN THE NEW INTERFACE SELECT “ACTIVE” UNDER ASSIGNMENT TYPE, MAINTAIN CHECK THE OPTION “PERMANENTLY ASSIGNED” AND PROVIDE A JUSTIFICATION TO ENABLE THE “ASSIGN” BUTTON

## STEPS

The screenshot shows the Azure portal interface. At the top, there is a search bar with the text "Azure acti". Below the search bar, a navigation bar includes tabs for "All", "Services (92)", "Resources", "Resource Groups", "Marketplace", and "Documentation". A sub-menu for "Azure Active Directory" is open under the "Services" tab. The main content area displays sections for "Start with an Azure free trial", "Manage Azure Active Directory", and "Access student benefits". Below these sections is a "Azure services" section with icons for "Create a resource", "Azure Active Directory", "Azure Information...", "Microsoft Purview...", "Azure AD B2C", "Azure AD Privileged...", "Help + support", "Microsoft Sentinel", "Function App", and "More services". The "Resources" section at the bottom shows a table with columns for "Name", "Type", and "Last Viewed". A message indicates "No resources have been viewed recently" with a "View all resources" button.

## STEPS

The screenshot shows the Azure Active Directory Overview page for the tenant 'Kaz Demos'. The left sidebar lists various management options like Users, Groups, External Identities, and Roles and administrators, with 'Roles and administrators' highlighted. The main area displays basic information about the tenant, including its name, tenant ID, primary domain, license, and user/group/application/device counts. It also features two warning cards about MFA Server deprecation and TLS/3DES deprecation.

**Kaz Demos | Overview**

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center! [Learn more](#)

**Overview** [Monitoring](#) [Properties](#) [Tutorials](#)

Search your tenant

**Basic information**

Name	Kaz Demos	Users	36
Tenant ID	ac1dff03-7e0e-4ac8-a4c9-9b38d24f062c	Groups	71
Primary domain	kazdemos.org	Applications	9
License	Azure AD Premium P2	Devices	12

**Alerts**

**Upcoming MFA Server deprecation**  
Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid any service impact.  
[Learn more](#)

**Upcoming TLS 1.0, 1.1 and 3DES deprecation**  
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.  
[Learn more](#)

## STEPS

Home > Kaz Demos | Roles and administrators >

### Roles and administrators | All roles

Kaz Demos - Azure Active Directory



+ New custom role

Delete custom role

Download assignments

Refresh

Preview features

Got feedback?

#### All roles

#### Diagnose and solve problems

#### Activity

#### Access reviews

#### Audit logs

#### Troubleshooting + Support

#### New support request

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

<input type="checkbox"/> B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	Built-in
<input type="checkbox"/> B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	Built-in
<input type="checkbox"/> Billing Administrator	Can perform common billing related tasks like updating payment information.	Built-in
<input type="checkbox"/> Cloud App Security Administrator	Can manage all aspects of the Cloud App Security product.	Built-in
<input type="checkbox"/> Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	Built-in
<input type="checkbox"/> Cloud Device Administrator	Limited access to manage devices in Azure AD.	Built-in
<input checked="" type="checkbox"/> Compliance Administrator	Can read and manage compliance configuration and reports in Azure AD and Microsoft 365.	Built-in
<input type="checkbox"/> Compliance Data Administrator	Creates and manages compliance content.	Built-in
<input type="checkbox"/> Conditional Access Administrator	Can manage Conditional Access capabilities.	Built-in
<input type="checkbox"/> Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	Built-in
<input type="checkbox"/> Desktop Analytics Administrator	Can access and manage Desktop management tools and services.	Built-in
<input type="checkbox"/> Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	Built-in
<input type="checkbox"/> Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	Built-in

## STEPS

Home >

### Compliance Administrator | Assignments

Privileged Identity Management | Azure AD roles

Add assignments Settings Refresh Export Got feedback?

Manage

Assignments Description Role settings

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	Start time	End time	
Compliance Administrator								
Mou	m@kazdemos.org	User	Directory	Direct	Assigned	-	Permanent	
Darrer	ll@kazdemos.o	User	Directory	Direct	Assigned	-	Permanent	
Vinicic	@kazdemos.org	User	Directory	Direct	Assigned	-	Permanent	
Fem	i@kazdemos.org	User	Directory	Direct	Assigned	-	Permanent	
N	N	ui@kazdemo	User	Directory	Direct	Assigned	-	Permanent
N.	I	jl@kazdemos.org	User	Directory	Direct	Assigned	-	Permanent
D	c	ot@kazdemos.org	User	Directory	Direct	Assigned	-	Permanent
Mic.	sports 701	13-d3	Service principal	Directory	Direct	Assigned	10/11/2022, 7:09:36 PM	Permanent
M.	Sen 096	0c0-d	Service principal	Directory	Direct	Assigned	12/12/2022, 5:37:55 PM	Permanent
Test	col 6	-9831-d	Service principal	Directory	Direct	Assigned	10/27/2022, 1:26:04 PM	Permanent

## STEPS

Home > Compliance Administrator | Assignments >

### Add assignments

Privileged Identity Management | Azure AD roles

**Membership**   Setting

**Resource**  
Kaz Demos

**Resource type**  
Directory

**Select role** ⓘ  
Compliance Administrator

**Scope type** ⓘ  
Directory

**Select member(s) \*** ⓘ  
No member selected

Next >   Cancel   Select

**Select a member**  
Privileged Identity Management | Azure AD roles

Only groups eligible for role assignment are displayed. [Learn more](#)

MPARR  
MPARR - Collector for Sentinel  
M- 0 -a0 Jef9 Selected

**Selected items**

M- MPARR - Collector for Sentinel  
096e4 -a0 Jef9 Remove



## STEPS

Home > Compliance Administrator | Assignments >

### Add assignments ...

Privileged Identity Management | Azure AD roles

Membership    Setting

Assignment type ⓘ

Eligible

Active

Maximum allowed assignment duration is permanent.

Permanently assigned

Assignment starts  
12/30/2022  7:57:35 PM

Assignment ends  
06/28/2023  7:57:35 PM

Enter justification \*

Unattended script for Microsoft Purview Advanced Rich Reports (MPARR) collector ✓

## CONFIGURE THE SCRIPT

- INSTALL **POWERSHELL V7**
- CREATE A LOCAL FOLDER UNDER C:\ LIKE AS "**COLLECTOR**"
- UNZIP THE FILE "**MPARR COLLECTOR.ZIP**" IN THAT FOLDER
- OPEN THE FILE "**LACONFIG.JSON**" AND COMPLETE WITH THIS INFORMATION:
  - **ENCRYPTEDKEYS**: "FALSE" (TO USE CHECK [HERE](#), THIS CAN BE USED TO ENCRYPT THE KEYS STORED IN THIS FILE)
  - **APPCLIENTID**: APPLICATION (CLIENT) ID FROM APP REGISTRATION STEP
  - **CLIENTSECRETVALUE**: SECRET KEY FROM CERTIFICATES AND SECRETS UNDER APP REGISTRATION STEP
  - **TENANTGUID**: TENANT ID FROM APP REGISTRATION STEP
  - **TENANTDOMAIN**: PRINCIPAL DOMAIN IN THE TENANT
  - **LA\_CUSTOMERID**: WORKSPACE ID FROM LOGS ANALYTICS (HERE CAN BE USED SENTINEL WORKSPACE)
  - **LA\_SHAREDKEY**: PRIMARY KEY FROM LOGS ANALYTICS (HERE CAN BE USED SENTINEL WORKSPACE)
  - **CLOUD**: USED TO SELECT THE KIND OF TENANT, THIS PERMIT USES THE RIGHT URL FOR THE COLLECTOR (SEE NOTES)
  - **CERTIFICATETHUMB**: CERTIFICATE THUMBPRINT FROM A SELF SIGNED CERTIFICATE
  - **ONMICROSOFTURL**: TENANT DOMAIN IN FORMAT <TENANT.ONMICROSOFT.COM>
  - **RMSLOGS**: THIS WILL BE USED FOR THE GET-RMSDATA SCRIPT TO CAPTURE INFORMATION FROM AIP SERVICE API
  - **OUTPUTLOGS**: SELECT WHERE YOUR LOGS WILL BE RECORDED
- SAVE THE CHANGES



## CONFIGURE THE SCRIPT

- ON THE SAME FOLDER
- OPEN THE FILE “**SCHEMA.JSON**” AND MAKE CHANGES IF YOU WANT TO AVOID DOWNLOAD CERTAIN KIND OF INFORMATION:
  - ACCORDING TO [THIS](#) INFORMATION, ALL THE INFORMATION COLLECTED ON THE DIFFERENT OFFICE 365 MANAGEMENT API SCHEMAS ARE COLLECTED ON 5 CONTENT BLOBS, THESE ARE:
    - AUDIT.AZUREACTIVEDIRECTORY
    - AUDIT.EXCHANGE
    - AUDIT.SHAREPOINT
    - AUDIT.GENERAL (INCLUDES ALL OTHER WORKLOADS NOT INCLUDED IN THE PREVIOUS CONTENT TYPES)
    - DLP.ALL (DLP EVENTS ONLY FOR ALL WORKLOADS)
  - TO MAKE ANY CHANGES TO AVOID CERTAIN INFORMATION THE VALUE “TRUE” NEED TO CHANGED TO “FALSE”
- SAVE THE CHANGES

## CONFIGURE TASK SCHEDULER

- OPEN **TASK SCHEDULER**
- GO TO TASK SCHEDULER LIBRARY
- UNDER ACTIONS CLICK **CREATE TASK\***
  - ON GENERAL TAB
  - SET A NAME
  - UNDER SECURITY OPTIONS CHANGE TO RUN WHETHER USERS IS LOGGED ON OR NOT
  - ON TRIGGERS TAB
  - ON SETTINGS SELECT DAILY
  - ON ADVANCED SETTINGS SET REPEAT TASK EVERY IN THIS CASE 10 MINUTES, CAN BE SET EVERY HOUR, AND FOR A DURATION OF INDEFINITELY
  - ON ACTIONS TAB
  - CLICK NEW...
  - UNDER PROGRAM/SCRIPT LOOKING FOR POWERSHELL 7 APPLICATION, NORMALLY IS IN THIS PATH "C:\PROGRAM FILES\POWERSHELL\7\PWSH.EXE"
  - UNDER ADD ARGUMENTS SELECT THE PATH TO THE SCRIPT LIKE AS ""C:\COLLECTOR\KAZDEMOS\RUN\_ME.PS1""
  - SELECT OK AND LOCAL CREDENTIALS WILL BE REQUIRED
  - THE SCRIPT CAN BE EXECUTED PRESSING RUN OPTION

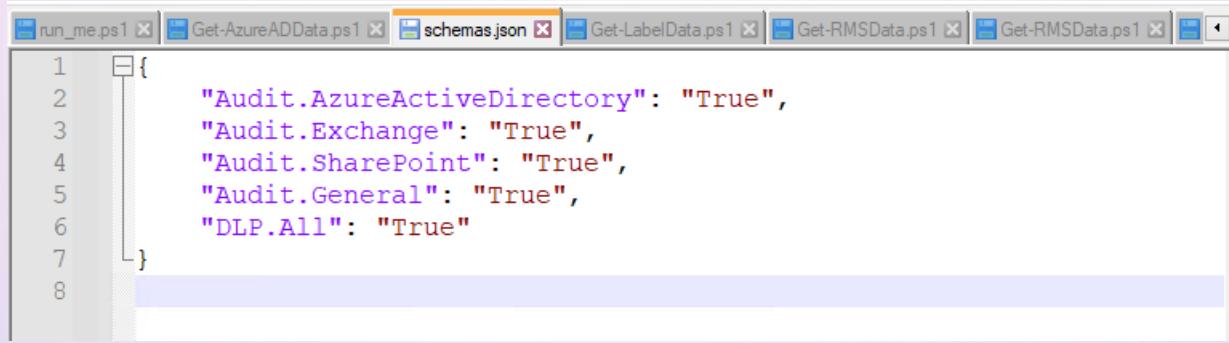
\*Using the same process can be created a new task under task scheduler to execute the PowerShell script **Get-RMSData.ps1**, is required to execute on PowerShell v5



## STEPS

```
1 {  
2     "EncryptedKeys": "False",  
3     "AppClientID": "70f-205-4f-83c0-20",  
4     "ClientSecretValue": "i5o0jRZEVbKs",  
5     "TenantGUID": "a3-7e-48-a9-92c",  
6     "TenantDomain": "kazdemos.org",  
7     "LA_CustomerID": "5d4c-71c-41i-8bf-04",  
8     "LA_SharedKey": "kNIDKC",  
9     "Cloud": "Commercial",  
10    "CertificateThumb": "180000000000000000000000000000000F4179BCD9",  
11    "OnmicrosoftURL": "M3.onmicrosoft.com",  
12    "RMSLogs": "c:\\Collector\\Script2.0\\RMSLogs\\",  
13    "OutPutLogs": "Logs\\"  
14}  
15
```

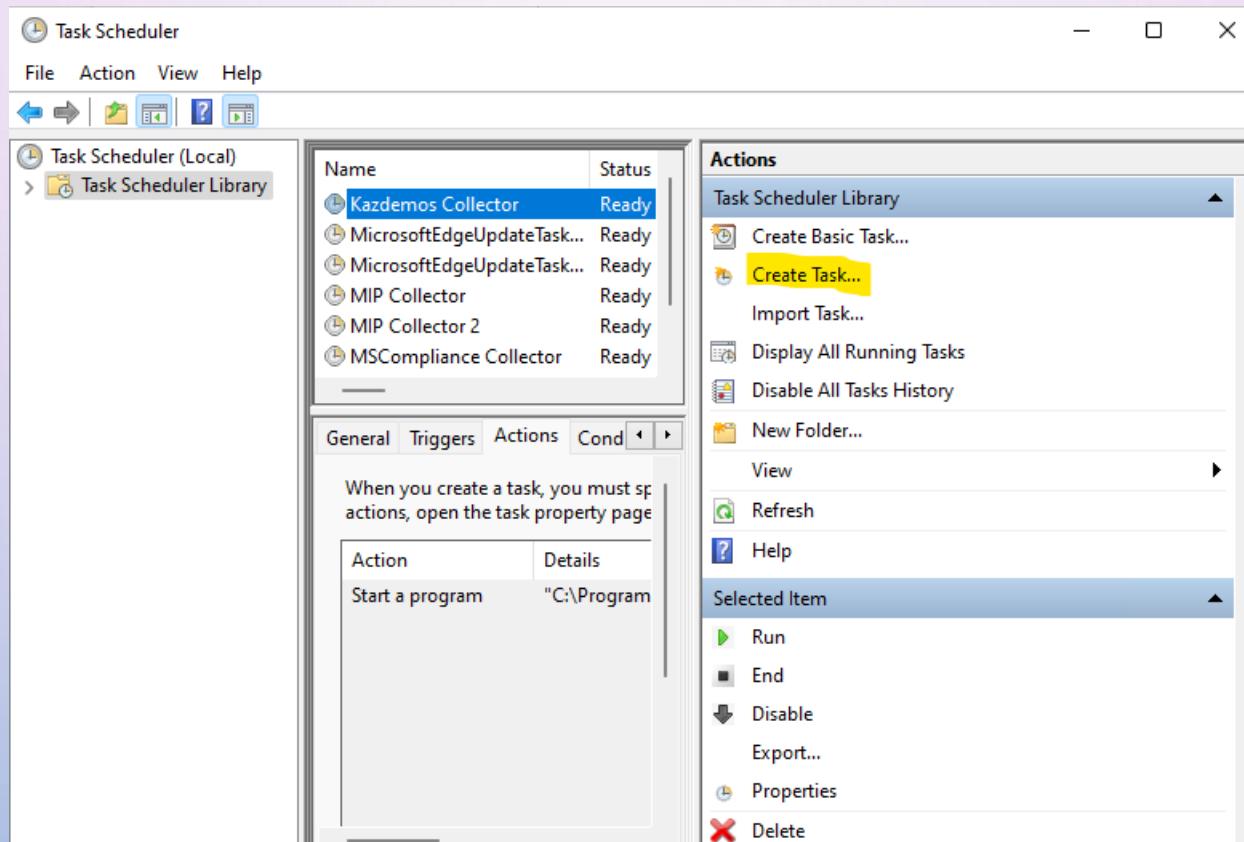
## STEPS



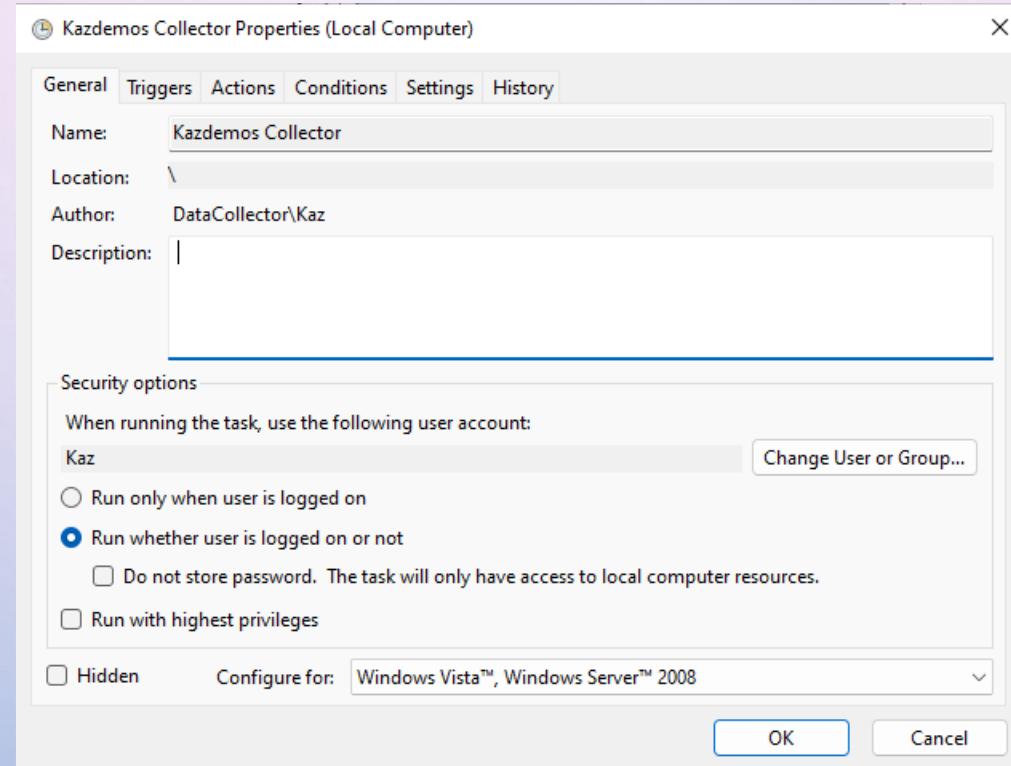
```
1  {
2      "Audit.AzureActiveDirectory": "True",
3      "Audit.Exchange": "True",
4      "Audit.SharePoint": "True",
5      "Audit.General": "True",
6      "DLP.All": "True"
7  }
```

# WORKSTATION OR SERVER

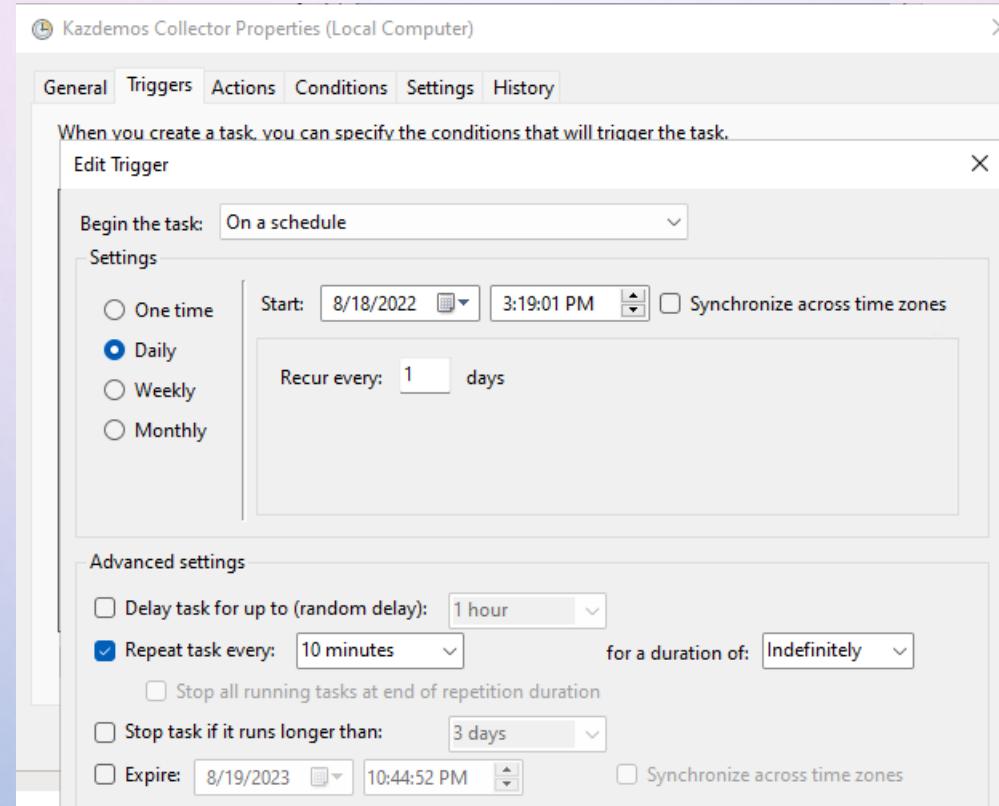
## STEPS



## STEPS

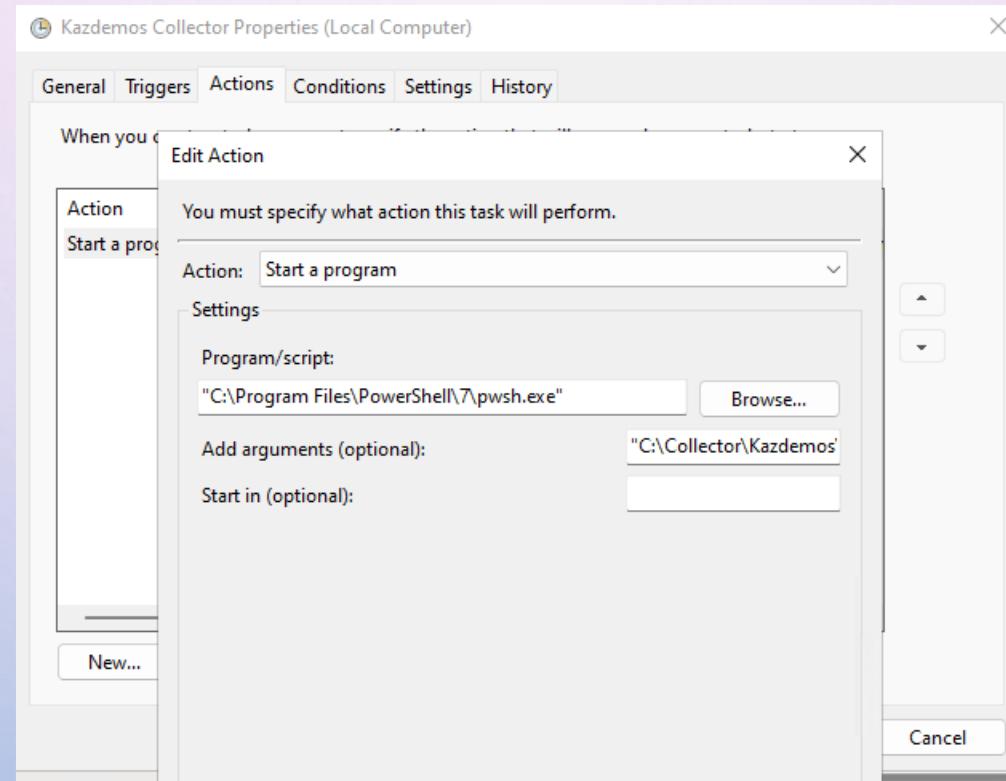


## STEPS

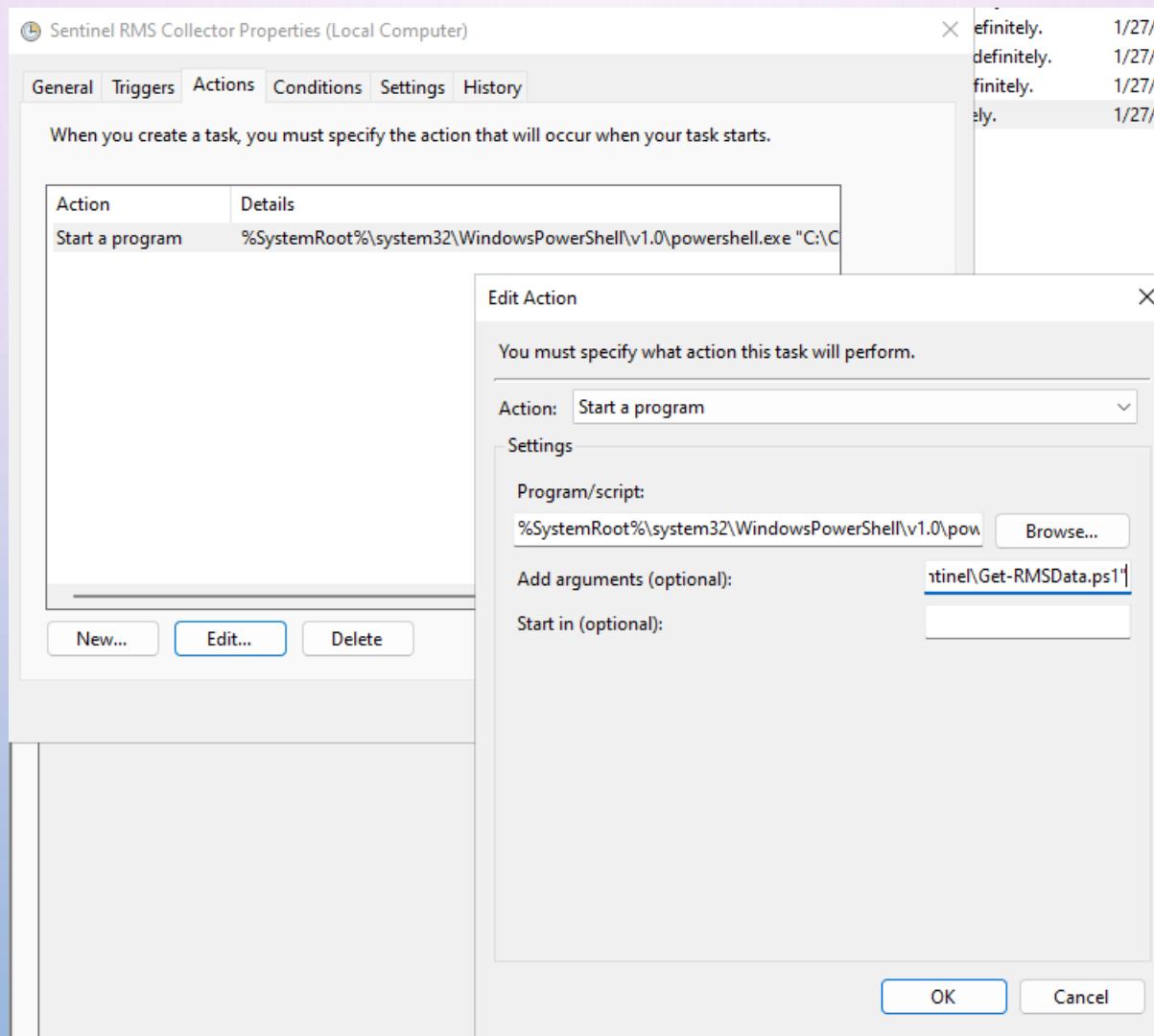


# WORKSTATION OR SERVER

## STEPS

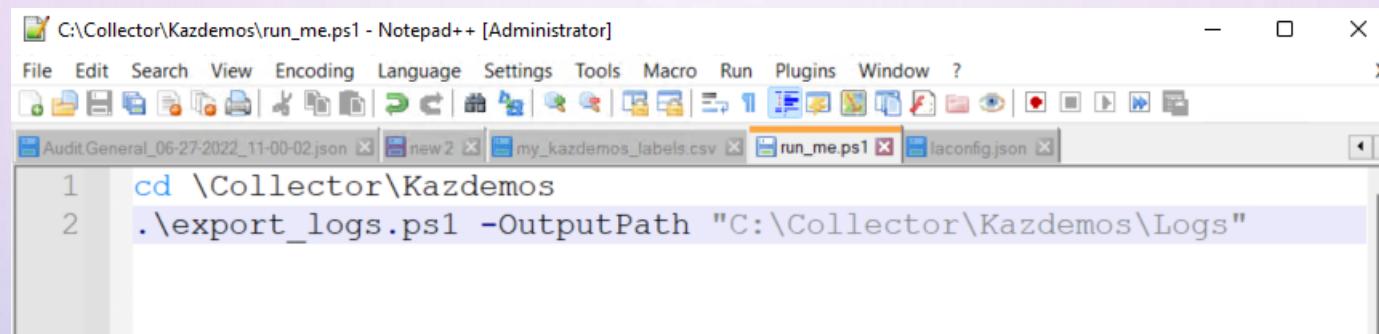


## STEPS (GET-RMSDATA.PS1 NEEDS TO BE EXECUTE WITH POWERSHELL V5)



## TO EXECUTE THE SCRIPT WITH PARAMETERS

- CREATE A **RUN\_ME.PS1** FILE IN THIS WAY, AND THEN REPLACE THE SCRIPT USED UNDER TASK SCHEDULER



```
C:\Collector\Kazdemos\run_me.ps1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Audit.General_06-27-2022_11-00-02.json new 2 my_kazdemos_labels.csv run_me.ps1 laconfig.json
1 cd \Collector\Kazdemos
2 .\export_logs.ps1 -OutputPath "C:\Collector\Kazdemos\Logs"
```

- ADDITIONAL PARAMETERS ARE AVAILABLE AS A COMMENTS UNDER “EXPORT\_LOGS.PS1”, THAT OPTIONS CAN BE USED TO FILTER SOME **SPECIFIC OPERATIONS**, OR CHANGE LOG DIRECTORY, OR SET ONLY TO EXPORT TO LOCAL FILES. THESE FILTERS ARE:
  - FILTERAUDITAZUREACTIVEDIRECTORY
  - FILTERAUDITEXCHANGE
  - FILTERAUDITSHAREPOINT
  - FILTERAUDITGENERAL
  - FILTERDLPALL
- ALL THE FILTER AVAILABLE ARE EXPLAINED ON THE PRINCIPAL SCRIPT HEADER

# TO ENCRYPT AZURE AD APP KEY, WORKSPACE KEY AND CERTIFICATE THUMBPRINT DO THIS:

- OPEN LACONFIG.JSON FILE AND DO\* THIS ACTIONS:

- UNDER “ENCRYPTEDKEYS” CHANGE “FALSE” BY “TRUE”

**COPY THE VALUE FOR “CLIENTSECRETVALUE” AND EXECUTE ON POWERSHELL THIS CMDLET:**

- PS C:\> "CLIENTSECRETVALUE\*\*" | CONVERTTO-SECURESTRING -ASPLAINTEXT -FORCE | CONVERTFROM-SECURESTRING
- REPLACE THE VALUE ON LACONFIG.JSON WITH THE NEW STRING

**COPY THE VALUE FOR “LA\_SHAREDKEY” AND EXECUTE ON POWERSHELL THIS CMDLET:**

- PS C:\> "LA\_SHAREDKEY\*\*" | CONVERTTO-SECURESTRING -ASPLAINTEXT -FORCE | CONVERTFROM-SECURESTRING
- REPLACE THE VALUE ON LACONFIG.JSON WITH THE NEW STRING

**COPY THE VALUE FOR “CERTIFICATETHUMB” AND EXECUTE ON POWERSHELL THIS CMDLET:**

- PS C:\> "CERTIFICATETHUMB\*\*" | CONVERTTO-SECURESTRING -ASPLAINTEXT -FORCE | CONVERTFROM-SECURESTRING
- REPLACE THE VALUE ON LACONFIG.JSON WITH THE NEW STRING

The screenshot shows two windows side-by-side. On the left is a PowerShell window titled 'Administrator: PowerShell 7 (x64)' showing command-line output for generating a secure string from a client secret value. On the right is a Notepad++ window titled 'C:\Collector\Script2.0\laconfig.json' showing the contents of the JSON configuration file. The 'ClientSecretValue' field has been highlighted in yellow, indicating it was copied from the PowerShell output.

```

Administrator: PowerShell 7 (x64)
PS C:\Collector\MPIP Demo> "St...oU" | ConvertTo-SecureString -AsPlainText -Force | Con
vertFrom-SecureString
01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a107
000
1a5ca7f6704f1d7f28183860893557d84e4e9255767d6000000027365d67b323ea5r0285f6f992d7f45867338b723fabee
c8410848f3c62736c2f7b
ac48cb19ce941c4d5dc7ad3c6fc5f005adfd5b37f
b98440000008f9b24451bd7f87d641150a9fe54f7808135890e72a55674a6a3f8001718fd07155439e4855e24f3fb
86770b453988d618102e265
c0fe8bce1f32b00caa98
PS C:\Collector\MPIP Demo> "74T...n1UnQ==" | ConvertTo-SecureString -AsPlainText -Force | ConvertFrom-SecureString
01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814
000038760a927b866b3c635c1b47cf24084ff7a747713608759b99a2c0e77b05a54000000000e800000000200002000000517e1587bf1b011b78
17c3906c2dd1a69eb2094b6397
805222a739b94aff548e571351e3fab8e533be66fe71a387ea72820d142a87c65fef6e24a39d342ea48148e98992b4252eb9d61660f5537dc5ee7e2
3529da83845f39b5c54c3349a90f9f5b5ada526fef786307062feb8c8f3411026475be999a9841fe48
070909b6725dec4b1f1add282f3a76260b114868ccae088c28c9c433774d09cfe9b0db7c2d0ffcf8c58ec35b64b
PS C:\Collector\MPIP Demo>

```

```

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 4 run_me.ps1 new 5 Get-auditLogs.ps1 export_logs.ps1 Get-LabelData.ps1 laconfig.json
1 {
2   "EncryptedKeys": "True",
3   "AppClientID": "701af...a3d5f20",
4   "ClientSecretValue": "01000000d08c9ddf0115d1118c7a00c04fc297eb01
5   "TenantGUID": "ac1d...38d24f062c",
6   "TenantDomain": "kazdemos.org",
7   "LA_CustomerID": "bd285...9731c3",
8   "LA_SharedKey": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000
9   "CertificateThumb": "01000000d08c9ddf0115d1118c7a00c04fc297eb010
10  "OnmicrosoftURL": "M3...36.onmicrosoft.com"
11 }
12

```

\*This action must be executed with the same account used to run the script

\*\*Use the key value



### SELECT YOUR TENANT TYPE BETWEEN ENTERPRISE, GCC, GCCH OR DOD

- SELECT TENANT TYPE WAS ADDED TO “**LACONFIG.JSON**” FILE UNDER “**CLOUD**” ATTRIBUTE
- THE POSSIBLE VALUES ARE:
  - **COMMERCIAL** - COMMERCIAL CLOUD
  - **GCC** - GOVERNMENT COMMUNITY CLOUD
  - **GCCH** - GOVERNMENT COMMUNITY HIGH CLOUD
  - **DOD** - DEPARTMENT OF DEFENSE CLOUD

## OBTAİN YOUR LABEL LIST WITH IDS AND SEND TO LOGS ANALYTICS

- PLEASE COMPLETE FIRST ALL THIS [STEPS](#), OFFICE 365 EXCHANGE ONLINE API IS USED TO OBTAIN THE NEXT INFORMATION
- THE DATA STORED ON API SCHEMAS CONTAINS ONLY THE ID OF THE LABELS, FOR THAT REASON IS REQUIRED HAVE A MATRIX BETWEEN IDS AND DISPLAY NAMES, THE SCRIPT USED HERE TAKE THE INFORMATION FROM INFORMATION PROTECTION SERVICE AND IMPORT THE DATA IN LOGS ANALYTICS.
- TO EXECUTE THIS SCRIPT PLEASE [COMPLETE THESE STEPS](#) 1<sup>ST</sup>.
- COPY THE SCRIPT GET-LABELDATA.PS1 TO THE SAME FOLDER WHERE THE LACONFIG.JSON FILE IS LOCATED, VALIDATE THAT YOU HAVE THE LAST VERSION OF THIS FILE CONTAINING CERTIFICATE THUMBPRINT AND ONMICROSOFT URL
- IF YOU HAVE AN ERROR TO EXECUTE, VALIDATE THAT THE CERTIFICATE WAS IMPORTED IN THE MACHINE USED TO EXECUTE THIS SCRIPT
- HOW TO CONSUME THROUGH POWER BI, [CLICK HERE](#).

# WORKSTATION - POWERSHELL

## STEPS

```
Administrator: PowerShell 7 (x64)
PS C:\Collector\Script2.0> .\Get-LabelData.ps1
WARNING: Your connection has been redirected to the following URI: "https://nam10b.ps.compliance.protection.outlook.com/
PowerShell-UserId?BasicAuthToOAuthConversion=true;PSVersion=7.2.6"
    37 rows returned by Get-Label
    37 rows written to Log Analytics workspace https://bd285ff7-1a38-4306-adaf-a367669731c3.ods.opinsights.azure.com/api/
logs?api-version=2016-04-01
PS C:\Collector\Script2.0>
```



## CREATE A TABLE IN LOGS ANALYTICS WITH PRODUCT NAMES AND SERVICE PLAN IDENTIFIERS FOR LICENSING

- WHEN USER LICENSING DATA IS EXPORTED, A SPECIAL NAMES ARE USED AND DOESN'T MATCH WITH KNOWN PRODUCTS, THESE STEPS HELPS TO CREATE A MATRIX FOR THAT PURPOSE.
- DOWNLOAD THE LATEST UPDATED PRODUCT LIST FROM [HERE](#) AND SAVE THE FILE IN A KNOWN FOLDER.
- USING THE SCRIPT EXPORTCSV2LA.PS1 YOU CAN IMPORT THE DATA TO LOGS ANALYTICS, TO DO THAT, EXECUTE THE SCRIPT IN THIS WAY:

```
PS C:\COLLECTOR> .\EXPORTCSV2LA.PS1 -FILENAME ".\PRODUCT NAMES AND SERVICE PLAN IDENTIFIERS  
FOR LICENSING.CSV"-TABLENAME "MSPRODUCTS"
```

- AFTER EXECUTING THE SCRIPT CAN TAKE BETWEEN 5 TO 10 MINUTES TO DISPLAY THE NEW TABLE UNDER LOGS ANALYTICS
- HOW TO CONSUME THROUGH POWER BI, [CLICK HERE](#).

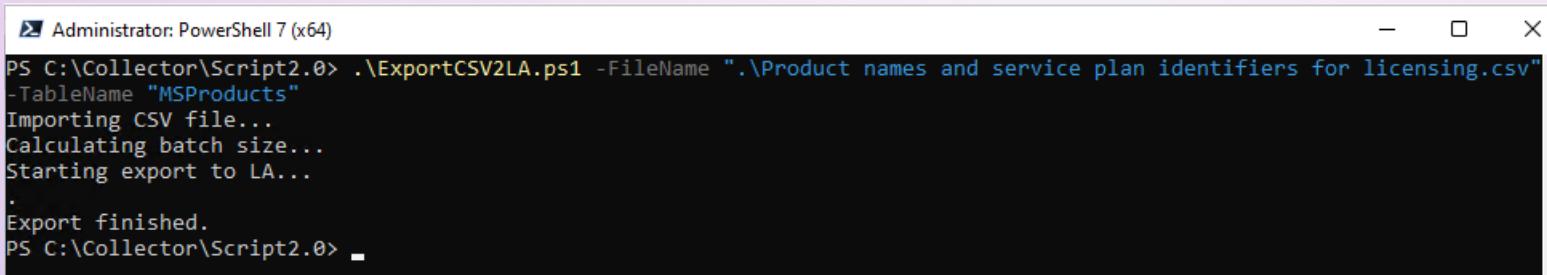
\*<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-service-plan-reference>

\*\*Depending on the Logs Analytics workspace retention this script will be required to execute continuously(monthly for a 30 days retention period) to don't lose that information

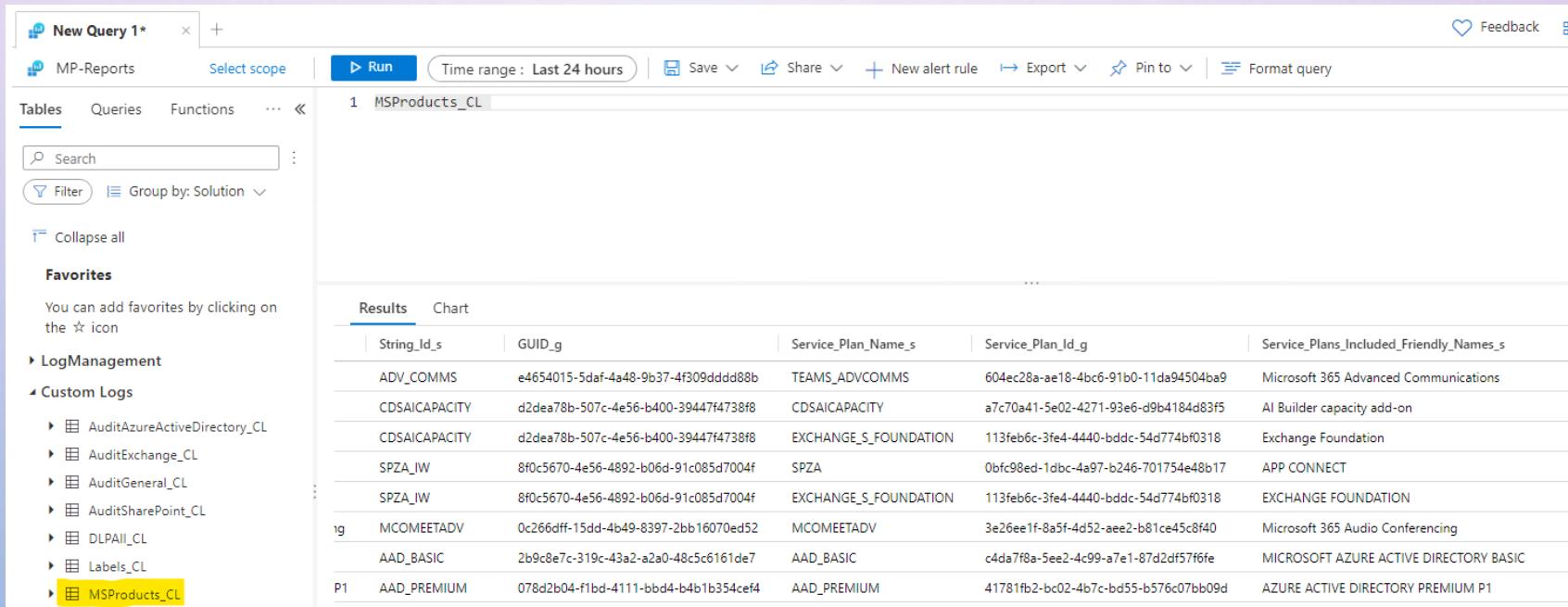
\*\*\* Power BI templates use the table name called "MSProducts" any change to this name, need to make the change on Power BI queries



## STEPS



```
Administrator: PowerShell 7 (x64)
PS C:\Collector\Script2.0> .\ExportCSV2LA.ps1 -FileName ".\Product names and service plan identifiers for licensing.csv"
-TableName "MSProducts"
Importing CSV file...
Calculating batch size...
Starting export to LA...
.
Export finished.
PS C:\Collector\Script2.0>
```



New Query 1\*

MP-Reports Select scope Run Time range: Last 24 hours Save Share New alert rule Export Pin to Format query

Tables Queries Functions ...

Search Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the icon

LogManagement

Custom Logs

- AuditAzureActiveDirectory\_CL
- AuditExchange\_CL
- AuditGeneral\_CL
- AuditSharePoint\_CL
- DLPAll\_CL
- Labels\_CL
- MSProducts\_CL**

1 MSProducts\_CL

Results Chart

String_Id_s	GUID_g	Service_Plan_Name_s	Service_Plan_Id_g	Service_Plans_Included_Friendly_Names_s
ADV_COMM	e4654015-5daf-4a48-9b37-4f309dd88b	TEAMS_ADVCOMMS	604ec28a-ae18-4bc6-91b0-11da94504ba9	Microsoft 365 Advanced Communications
CDSAICAPACITY	d2dea78b-507c-4e56-b400-39447f4738f8	CDSAICAPACITY	a7c70a41-5e02-4271-93e6-d9b4184d83f5	AI Builder capacity add-on
CDSAICAPACITY	d2dea78b-507c-4e56-b400-39447f4738f8	EXCHANGE_S_FOUNDATION	113feb6c-3fe4-4440-bddc-54d774bf0318	Exchange Foundation
SPZA_IW	8f0c5670-4e56-4892-b06d-91c085d7004f	SPZA	0bfc98ed-1dbc-4a97-b246-701754e48b17	APP CONNECT
SPZA_IW	8f0c5670-4e56-4892-b06d-91c085d7004f	EXCHANGE_S_FOUNDATION	113feb6c-3fe4-4440-bddc-54d774bf0318	EXCHANGE FOUNDATION
1g	0c266dff-15dd-4b49-8397-2bb16070ed52	MCOMEETADV	3e26ee1f-8a5f-4d52-aee2-b81ce45c8f40	Microsoft 365 Audio Conferencing
	AAD_BASIC	AAD_BASIC	c4da7f8a-5ee2-4c99-a7e1-87d2df57f6fe	MICROSOFT AZURE ACTIVE DIRECTORY BASIC
P1	AAD_PREMIUM	AAD_PREMIUM	41781fb2-bc02-4b7c-bd55-b576c07bb09d	AZURE ACTIVE DIRECTORY PREMIUM P1

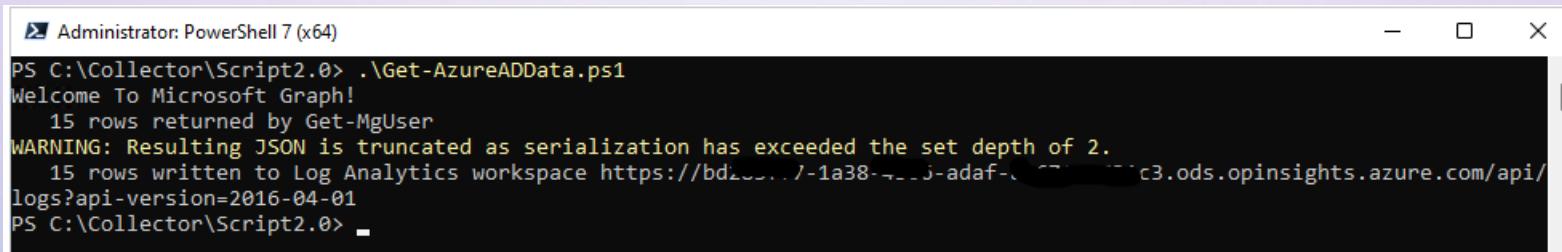
## LIST OF AZURE AD USERS WITH ATTRIBUTES AND LICENSING

- PLEASE COMPLETE FIRST ALL THIS [STEPS](#), MICROSOFT GRAPH API IS USED TO OBTAIN THE NEXT INFORMATION
- TO GENERATE A LIST OF AZURE AD USERS WITH SOME ATTRIBUTES LIKE COUNTRY, CITY, DEPARTMENT, JOB TITLE, OR OFFICE LOCATION, YOU NEED EXECUTE THE SCRIPT **GET-AZUREADDATA.PS1** PREVIOUSLY CHECK THAT YOU ARE USING THE LATEST **LACONFIG.JSON** FILE THAT CONTAIN THE ATTRIBUTE **CERTIFICATEHUMB**
- EXECUTE THE SCRIPT ON POWERSHELL 7 AND THAT IS.

```
PS C:\COLLECTOR> .\GET-AZUREADDATA.PS1
```

# POWERSHELL - AZURE AD USERS

## STEPS



```
Administrator: PowerShell 7 (x64)
PS C:\Collector\Script2.0> .\Get-AzureADData.ps1
Welcome To Microsoft Graph!
    15 rows returned by Get-MgUser
WARNING: Resulting JSON is truncated as serialization has exceeded the set depth of 2.
    15 rows written to Log Analytics workspace https://bd.../1a38-...-adaf-...-c3.ods.opinsights.azure.com/api/logs?api-version=2016-04-01
PS C:\Collector\Script2.0>
```



## LIST OF AZURE AD ROLES AND DOMAINS REGISTERED

- PLEASE COMPLETE FIRST ALL THIS [STEPS](#), MICROSOFT GRAPH API IS USED TO OBTAIN THE NEXT INFORMATION
- TO GENERATE A LIST OF AZURE AD ROLES, AND DOMAINS REGISTERED ON THE TENANT, YOU NEED EXECUTE THE SCRIPT **GET-AZUREADROLES.PS1** AND **GET-AZUREADDOMAINS.PS1**, PREVIOUSLY CHECK THAT YOU ARE USING THE LATEST **LACONFIG.JSON** FILE THAT CONTAIN THE ATTRIBUTE **CERTIFICATEHUMB**
- EXECUTE THE SCRIPT ON POWERSHELL 7 AND THAT IS.

```
PS C:\COLLECTOR> .\GET-AZUREADDOMAINS.PS1
```

```
PS C:\COLLECTOR> .\GET-AZUREADROLES.PS1
```

# POWERSHELL - AZURE AD USERS

## STEPS

```
Administrator: PowerShell 7 (x64)
PS C:\Collector\Sentinel> .\Get-AzureADRoles.ps1
Welcome To Microsoft Graph!
    17 rows returned by Get-MgDirectoryRole
Processing account Conditional Access Administrator 1/17
Processing account Privileged Role Administrator 2/17
Processing account Exchange Administrator 3/17
Processing account Cloud Device Administrator 4/17
Processing account Security Administrator 5/17
Processing account Global Reader 6/17
Processing account Intune Administrator 7/17
Processing account Security Reader 8/17
Processing account User Administrator 9/17
Processing account Reports Reader 10/17
Processing account Compliance Administrator 11/17
Processing account Azure Information Protection Administrator 12/17
Processing account Directory Readers 13/17
Processing account Global Administrator 14/17
Processing account Application Administrator 15/17
Processing account Azure AD Joined Device Local Administrator 16/17
Processing account Cloud App Security Administrator 17/17
    17 rows written to Log Analytics workspace https://f7e2ed[REDACTED]5d953.ods.opinsights.azure.com/api/logs?api-version=2016-04-01
PS C:\Collector\Sentinel> .\Get-AzureADDomains.ps1
Welcome To Microsoft Graph!
    3 rows returned by Get-MgDomains
Processing account M365x089236.onmicrosoft.com 1/3
Processing account kazdemos.org 2/3
Processing account ms-mparr.com 3/3
    3 rows written to Log Analytics workspace https://f7e2ed[REDACTED].ods.opinsights.azure.com/api/logs?api-version=2016-04-01
PS C:\Collector\Sentinel>
```



## CONNECT TO LOGS STORED IN YOUR WORKSPACE

- OPEN [HTTPS://PORTAL.AZURE.COM](https://portal.azure.com)
- LOOK FOR LOG ANALYTICS WORKSPACES
  - SELECT YOUR WORKSPACE PRESSING OVER THE NAME
  - ON THE NEW BLADE UNDER GENERAL CATEGORY PRESS LOGS MENU
  - CLOSE THE POP-UP WINDOWS
  - LOOK FOR CUSTOM LOGS UNDER TABLES AND PRESS THE ARROW TO SHOW ALL THE TABLES
  - IF THE SCRIPT IS RUNNING WELL AND THE TENANT HAVE A NORMAL USE THESE 5 TABLES(BASED ON THE PRINCIPAL SCRIPT) WILL BE APPEAR\* UNDER CUSTOM LOGS:
    - **AUDITAZUREACTIVE DIRECTORY\_CL**
    - **AUDITEXCHANGE\_CL**
    - **AUDITGENERAL\_CL**
    - **AUDITSHAREPOINT\_CL**
    - **DLPALL\_CL**
  - OTHER TABLES ARE ADDED FROM OTHER SCRIPTS:
    - **AZUREADUSERS\_CL**
    - **AZUREADROLES\_CL**
    - **AZUREADDOMAINS\_CL**
    - **LABELS\_CL**
    - **MSPRODUCTS\_CL**
    - **RMSDATA\_CL**
    - **RMSDATADETAILS\_CL**

\*The first time that the script is running the tables can take between 5 to 15 minutes to appear under Custom Logs, if as an example no DLP rules are applied or Exchange is not used the tables will not appear until an operation is recorded.



## EXPORT TO USE FROM POWER BI

- THE NEXT STEPS ARE REQUIRED TO DO FOR EACH TABLE (5):
  - DOUBLE CLICK IN TABLE NAME, THAT ACTION WILL BE PUT THE NAME OF THE TABLE ON QUERY SPACE
  - PRESS RUN BUTTON (IS NOT REQUIRE MAKE CHANGES OVER TIME RANGE)
  - AFTER PRESSING THE QUERY WILL BE RUNNING AND SOME RESULTS WILL BE APPEARED AT RESULT AREA.
  - THE EXPORT OPTION WILL BE AVAILABLE, PRESS AND SELECT EXPORT TO POWER BI (M QUERY)
  - THE PREVIOUS STEP WILL GENERATE A TXT FILE, SAVE AND RENAME THE FILE IN A KNOW LOCATION USING THE TABLE NAME AS A FILENAME.
  - UNDER THE SAME QUERY, BELOW TABLE NAME ADD THE NEXT QUERY:

```
| WHERE TIMEGENERATED > NOW(-730D)  
| SUMMARIZE BY  
    YEAR = DATETIME_PART('YEAR',TIMEGENERATED),  
    MONTH = DATETIME_PART('MONTH',TIMEGENERATED),  
    DAY = DATETIME_PART('DAY',TIMEGENERATED)
```
  - THE PREVIOUS WILL BE USED TO RESOLVE A DOWNLOAD LIMIT ON POWER BI, MORE INFORMATION IN THIS [LINK](#)
  - PRESS RUN BUTTON AND EXPORT TO POWER BI (M QUERY), SAME AS PREVIOUS STEP, AND ADD THE WORD “DATE” AS A PREFIX FOR FILENAME.
  - THE RESULTS WILL BE SHOW YEARS AND MONTHS FOR THE LAST 730 DAYS OF THE DATA COLLECTED, IN THIS CASE MAYBE ONLY 1 YEAR AND ONE MONTH.

## STEPS

The screenshot shows the Azure portal search results for "log Analytics". The search bar at the top contains the query "log Analytics". Below the search bar, there are several filter buttons: All (selected), Services (17), Marketplace (7), Documentation (20), Resources (0), and Resource Groups (0). The main search results are categorized under "Services", "Marketplace", and "Documentation".

**Services**

- Log Analytics query packs
- Log Analytics workspaces (highlighted)
- Activity log
- Stream Analytics clusters

**Marketplace**

- Log Analytics Workspace
- Azure Log Analytics Agent Health
- FortiAnalyzer Centralized Log Analytics
- HPE OneView for Azure Log Analytics (v1.4.0)
- Logz.io - Cloud Monitoring and Observability
- Cloud-Native Observability with Logz.io (LEGACY)
- SEEPATH-managed-azure

**Documentation**

- Overview of Log Analytics in Azure Monitor - Azure Monitor
- Create Log Analytics workspaces - Azure Monitor | Microsoft Docs

## STEPS

The screenshot shows the 'Log Analytics workspaces' page in the Azure portal. The top navigation bar includes 'Home >', the workspace name 'Log Analytics workspaces', and a 'mscompliance' tag. Below the navigation are standard actions: 'Create', 'Open recycle bin', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A search bar contains the filter 'Sentinel'. The main area displays a single workspace entry:

Name ↑	Resource group ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/> Sentinel	LAB	East US	Azure subscription 1

On the right side of the table, there are grouping and view settings: 'No grouping' and 'List view'. A three-dot ellipsis menu is also present.

## STEPS

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a navigation bar with 'Home > Log Analytics workspaces > Log Analytics work...'. Below it, a search bar and a 'Create' button are visible. A list of workspaces is shown, with 'Sentinel' selected. The main content area is titled 'Sentinel' and shows the 'Log Analytics workspace' details. It includes a 'Search' bar, a 'Delete' button, and a note about the migration of Log Analytics agents to Azure Monitor Agent. The 'Essentials' section displays resource group (move) as 'lab', status as 'Active', location as 'East US', subscription as 'Azure subscription 1', subscription ID as '1c2f...', and tags as 'Click here to add tags'. Below this, a 'Get started with Log Analytics' section provides information on collecting data from various sources and using a powerful query language. Two numbered steps are listed: '1 Connect a data source' and '2 Configure monitoring solutions'. Step 1 suggests connecting to Azure virtual machines (VMs), Windows and Linux Agents management, Storage account log, and System Center Operations Manager. Step 2 suggests adding monitoring solutions for insights into applications and services. At the bottom, a call-to-action 'Maximize your Log Analytics experience' is present.

Home > Log Analytics workspaces >

**Log Analytics work...** mscompliance

+ Create Open recycle bin ...

Sentinel

Name ↑↓

**Sentinel** ...

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Agents management

Legacy agents management

Custom logs

Computer Groups

Data export

Linked storage accounts

Network isolation

Tables

**General**

Workspace summary

Workbooks

**Logs**

Solutions

**Sentinel** Log Analytics workspace

Search

Delete

**i** The Log Analytics agents (MMA.OMS) used to collect logs from virtual machines and servers will no longer be supported after July 2020. Learn more about migrating to Azure Monitor Agent

Resource group (move) : lab

Status : Active

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : 1c2f...

Tags (edit) : Click here to add tags

### Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

**1 Connect a data source**

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)

Windows and Linux Agents management

Storage account log

System Center Operations Manager

**2 Configure monitoring solutions**

Add monitoring solutions that provide insights for applications and services in your environment

View solutions

Maximize your Log Analytics experience

# LOGS ANALYTICS WORKSPACE

## STEPS

The screenshot shows the Microsoft Sentinel Log Analytics workspace interface. On the left, there's a navigation sidebar with sections like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, there are options for Locks, Agents management, Legacy agents management, Custom logs, Computer Groups, Data export, Linked storage accounts, Network isolation, Tables, and General (Workspace summary, Workbooks, Logs, Solutions, Usage and estimated costs, Properties, Service Map). The 'Logs' item under General is highlighted with a yellow box. The main area has a search bar at the top, followed by a 'New Query 1' card with tabs for Tables, Queries, Functions, and a 'Run' button. Below this is a 'Tables' section with a search bar and filter options. A 'Favorites' section lists 'LogManagement', 'Microsoft Sentinel' (which is also highlighted with a yellow box), and 'Custom Logs'. The 'Custom Logs' section contains a list of log types: AuditAzureActiveDirectory\_CL, AuditExchange\_CL, AuditGeneral\_CL, AuditSharePoint\_CL, AzureADDomains\_CL, AzureADRoles\_CL, AzureADUsers\_CL, DLPAll\_CL, Labels\_CL, MSProducts\_CL, RMSData\_CL, and RMSDataDetails\_CL. To the right, there's a 'Queries History' section showing recent queries with their details and 'Run' buttons:

- DLPAll\_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation\_s) by Operation\_s  
1/30/2023, 1:23 PM | 4 results
- AuditSharePoint\_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation\_s) by Operation\_s  
1/30/2023, 1:22 PM | 47 results
- AuditGeneral\_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation\_s) by Operation\_s  
1/30/2023, 1:21 PM | 95 results
- AuditExchange\_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation\_s) by Operation\_s  
1/30/2023, 1:20 PM | 33 results
- AuditAzureActiveDirectory\_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation\_s) by Operation\_s  
1/30/2023, 1:14 PM | 38 results
- Labels\_CL  
1/27/2023, 3:38 PM | 422 results



## STEPS

The screenshot shows the Microsoft Log Analytics workspace interface. At the top, there's a navigation bar with tabs for 'Tables', 'Queries', 'Functions', and a search bar. Below the navigation bar, a sidebar titled 'Favorites' lists categories like 'LogManagement' and 'Custom Logs'. Under 'Custom Logs', several items are listed, with 'AuditAzureActiveDirectory\_CL' highlighted in yellow. The main area displays a table of query results with columns: TimeGenerated [UTC], Id\_g, Operation\_s, OrganizationId\_g, and RecordType\_d. The table contains five rows of data, each representing an audit log entry. A context menu is open over the first row, showing options like 'Export to CSV - all columns', 'Export to CSV - displayed columns', 'Export to Power BI (M query)', and 'Open in Excel'.

TimeGenerated [UTC]	Id_g	Operation_s	OrganizationId_g	RecordType_d
8/22/2022, 5:55:11.000 PM	cb1c1e...34f8200	UserLoginFailed	a...	62c 15
8/22/2022, 8:52:32.000 PM	b168bc...831ba00	UserLoginFailed	a...	62c 15
8/22/2022, 8:52:20.000 PM	c49e...7203b400	UserLoginFailed	a...	2c 15
8/22/2022, 5:55:15.000 PM	cb1c...00000000000000000000000000000000	UserLoggedIn	a...	00000000000000000000000000000000 15
8/22/2022, 8:52:20.000 PM	c49e...00000000000000000000000000000000	UserLoginFailed	a...	00000000000000000000000000000000 15

## STEPS

The screenshot shows the Microsoft Power BI Data Studio interface. On the left, there's a sidebar with 'Tables', 'Queries', and 'Functions' tabs, and a search bar. Below that are sections for 'Favorites' (with a note about adding favorites) and 'LogManagement' (listing 'AuditAzureActiveDirectory\_CL', 'AuditExchange\_CL', 'AuditGeneral\_CL', 'AuditSharePoint\_CL', and 'DLPAll\_CL'). The main area has a 'New Query 1\*' tab open, showing the following M language query:

```
1 AuditAzureActiveDirectory_CL  
2 | where TimeGenerated > now(-730d)  
3 | summarize by  
4 | Year = datetime_part('Year',TimeGenerated),  
5 | Month = datetime_part('Month',TimeGenerated)
```

The 'Run' button is highlighted in blue. To the right, there's a 'Time range: Set in query' dropdown, 'Save', 'Share', 'New alert rule', and 'Export' menus. The 'Export' menu is open, showing options: 'Export to CSV - all columns', 'Export to CSV - displayed columns', 'Export to Power BI (M query)' (which is highlighted in yellow), and 'Open in' (with 'Export to Power BI (M query)' as a sub-option). The results pane below shows a chart with 'Year' and 'Month' dimensions, with the value '2,022' for the year 2022 and month 8.

## EXPORT EXAMPLE

The screenshot shows a code editor window with the following content:

```
/*
The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel
and Power BI Desktop.
For Power BI Desktop follow the instructions below:
1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/
2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'
3) Paste the M Language script into the Advanced Query Editor and select 'Done'
*/


let AnalyticsQuery =
let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/5d642594-0883-4
[Query=[#"query"="AuditAzureActiveDirectory_CL
",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="P1D",#"prefer"="ai.response-thinning=true"],Timeout=#
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},
Columns = Table.FromRecords(DataTable[columns]),
ColumnsWithType = Table.Join(Columns, {"type"}, TypeMap , {"AnalyticsTypes"}),
Rows = Table.FromRows(DataTable[rows], Columns[name]),
Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3}}))
in
Table

Ln 1, Col 1           100%           Windows (CRLF)           UTF-8
```

## TO OBTAIN THE LATEST INFORMATION ABOUT LABELS

- LOGS ANALYTICS WORKS APPENDING DATA, FOR THAT REASON EVERY TIME THAT THE SCRIPT IS EXECUTED TO UPDATE THE INFORMATION, THAT DATA IS ADDED, IN THAT ORDER OF IDEAS IS IMPORTANT TO DOWNLOAD THE MOST RECENTLY INFORMATION, TO DO THAT EXECUTE THIS QUERY:

```
LABELS_CL  
| WHERE TIMEGENERATED > NOW(-730D)  
| PROJECT  
    DISPLAYNAME_S,  
    GUID_G,  
    PRIORITY_D,  
    PARENTLABELDISPLAYNAME_S,  
    TIMEGENERATED  
|SUMMARIZE MAX(TIMEGENERATED) BY GUID_G, DISPLAYNAME_S, PRIORITY_D, PARENTLABELDISPLAYNAME_S
```

- THEN EXPORT AS POWER BI(M QUERY) AND ADD TO THE REST OF QUERIES UNDER POWER BI DESKTOP

## TO OBTAIN THE LATEST INFORMATION ABOUT SERVICES PLAN AND PRODUCT NAMES

- LOGS ANALYTICS WORKS APPENDING DATA, FOR THAT REASON EVERY TIME THAT THE SCRIPT IS EXECUTED TO UPDATE THE INFORMATION, THAT DATA IS ADDED, IN THAT ORDER OF IDEAS IS IMPORTANT TO DOWNLOAD THE MOST RECENTLY INFORMATION, TO DO THAT EXECUTE THIS QUERY:

```
MSPRODUCTS_CL  
| WHERE TIMEGENERATED > NOW(-730D)  
| PROJECT  
    PRODUCT_DISPLAY_NAME_S,  
    GUID_G,  
    STRING_ID_S,  
    TIMEGENERATED  
|SUMMARIZE MAX(TIMEGENERATED) BY GUID_G, PRODUCT_DISPLAY_NAME_S, STRING_ID_S
```

- THEN EXPORT AS POWER BI(M QUERY) AND ADD TO THE REST OF QUERIES UNDER POWER BI DESKTOP

## TO OBTAIN THE LATEST INFORMATION ABOUT AZURE AD USERS AND LICENSING

LOGS ANALYTICS WORKS APPENDING DATA, FOR THAT REASON EVERY TIME THAT THE SCRIPT IS EXECUTED TO UPDATE THE INFORMATION, THAT DATA IS ADDED, IN THAT ORDER OF IDEAS IS IMPORTANT TO DOWNLOAD THE MOST RECENTLY INFORMATION, TO DO THAT EXECUTE THIS QUERY:

```
AZUREADINFO_CL  
| WHERE TIMEGENERATED > NOW(-730D) AND USERPRINCIPALNAME_S != ""  
| PROJECT  
    USERPRINCIPALNAME_S,  
    DISPLAYNAME_S,  
    ASSIGNEDLICENSES_S,  
    COUNTRY_S,  
    CITY_S,  
    JOBTITLE_S,  
    DEPARTMENT_S,  
    MAIL_S,  
    OFFICELOCATION_S,  
    TIMEGENERATED  
|SUMMARIZE MAX(TIMEGENERATED) BY USERPRINCIPALNAME_S, ASSIGNEDLICENSES_S, CITY_S, COUNTRY_S,  
DEPARTMENT_S, DISPLAYNAME_S, JOBTITLE_S, MAIL_S, OFFICELOCATION_S
```

THEN EXPORT AS POWER BI(M QUERY) AND ADD TO THE REST OF QUERIES UNDER POWER BI DESKTOP



## CONNECT TO LOGS STORED IN YOUR WORKSPACE\*

1. OPEN POWER BI DESKTOP
2. CLOSE THE INITIAL WELCOME POP-UP
3. GO TO GET DATA AND SELECT BLANK QUERY
4. UNDER POWER QUERY EDITOR WINDOW SELECT ADVANCED EDITOR
5. CLEAR THE EXAMPLE, OPEN “YOUR\_TABLE\_NAME.TXT” COPY AND PASTE ALL THE INFORMATION AND PRESS DONE
6. CREDENTIALS CAN BE REQUEST, OPEN AND SELECT ORGANIZATIONAL ACCOUNT, USER WITH READ PERMISSIONS OVER LOGS ANALYTICS WORKSPACE ARE REQUIRED
7. ON THE SAME WINDOW SELECT NEW SOURCE AND PRESS BLANK QUERY AGAIN
8. CLICK ON ADVANCED EDITOR AND CLEAR THE SAMPLE
9. OPEN “DATE\_YOUR\_TABLE\_NAME.TXT” COPY AND PASTE ALL THE INFORMATION AND PRESS DONE
10. AT TOP RIGHT UNDER PROPERTIES RENAME THE QUERY WITH YOUR TABLE NAME

\*Power BI templates are delivered with the script, these templates contains all the steps explained in this section, using the templates the next steps are not required



## POWER BI LIMIT RESOLVED

11. AT LEFT RIGHT CLICK OVER FIRST QUERY AND SELECT CREATE FUNCTION
12. A POP-UP APPEARS, PRESS CREATE
13. ASSIGN A NAME, LIKE AS DATA\_YOURTABLENAME AND PRESS OK
14. GO TO ADVANCED EDITOR AND CLICK IT
15. A POP-UP APPEARS, PRESS OK
16. MODIFY LINE 2 ADDING INSIDE SOURCE THIS ADDITIONAL DATA

SOURCE = (MONTH AS TEXT, YEAR AS TEXT) => LET ANALYTICSQUERY =

17. LOOKING ON THE SAME EDITOR THE VARIABLE #"**TIMESPAN**"="P1D", AND REPLACE P1D WITH THIS:

AUDITAZUREACTIVEDIRECTORY\_CL | WHERE DATETIME\_PART('MONTH',TIMEGENERATED) == "& MONTH &" AND  
DATETIME\_PART('YEAR',TIMEGENERATED) == "& YEAR &"

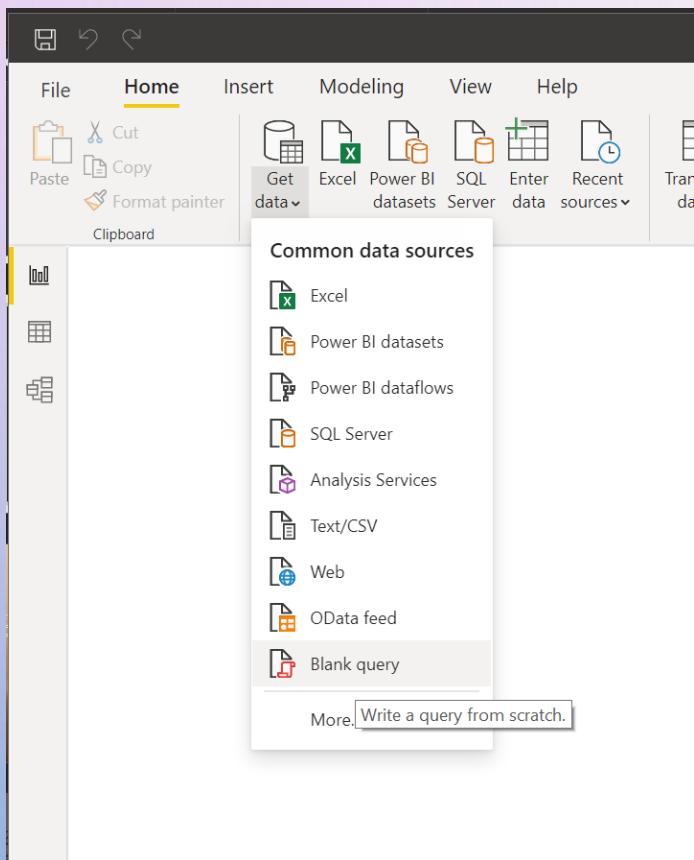
18. TAKE CARE ON PREVIOUS STEP TO USE THE CORRECT TABLE NAME AND PRESS DONE
19. FIRST QUERY CAN BE DELETED, ONLY THE DATE QUERY AND THE FUNCTION ARE REQUIRED
20. REPEAT FROM STEP 3 PRESSING NEW SOURCE AND BLANK QUERY FOR EACH TABLE NAME, AT THE FINAL YOU WILL HAVE 5 QUERIES AND 5 FUNCTIONS.

## POWER BI LIMIT RESOLVED

21. AFTER FINISH THE PREVIOUS STEPS WITH THE 5 TABLES IS REQUIRED MERGE THE QUERIES WITH THE FUNCTIONS, TO DO THAT PLEASE GO FORWARD WITH THE NEXT STEPS TAKING CARE IN EACH POINT
22. SELECT YOUR QUERY (THE ONE WITH YEAR AND MONTH AS RESULT), AT THE TOP SELECT THE TAB ADD COLUMN AND THEN PRESS INVOKE CUSTOM FUNCTION
23. ON THE POP-UP DON'T TOUCH NEW COLUMN NAME UNDER FUNCTION QUERY SELECT THE FUNCTION RELATED TO YOUR TABLE NAME; AFTER THAT 2 TEXT AREAS WILL BE APPEAR FILL MONTH WITH MONTH AND YEAR WITH YEAR AND PRESS OK
24. A NEW COLUMN WILL BE ADDED WITH THE CAPABILITY TO EXPAND PRESS THE ICON WITH 2 ARROWS ONE TO RIGHT AND THE OTHER TO LEFT LOCATED JUST RIGHT TO COLUMN NAME  

25. IN NEW WINDOW ALL COLUMNS RELATED TO THE ORIGINAL TABLE WILL BE APPEAR (SOMETIMES APPEAR AT BOTTOM AN OPTION TO LOAD MORE COLUMNS, IN THAT CASE PLEASE PRESS THAT OPTION) UNCHECK USE ORIGINAL NAME AS PREFIX
26. NOW ALL THE COLUMNS WILL BE ADDED BASED ON THE DATE, THAT STEP RESOLVE THE 500K LIMIT ON POWER BI, IF THE DATA IS TOO MANY A FIELD DAY CAN BE ADDED TO THE DATE QUERY.
27. IS IMPORTANT GO TO TIMEGENERATED COLUMN AND CHANGE THE DATA TYPE TO DATE/TIME/TIMEZONE THIS STEP IS RELEVANT TO APPLY FILTERS BASED ON TIME

# STEPS



Untitled - Power Query Editor

File Home Transform Add Column View Tools Help

Common data sources

- Excel
- Power BI datasets
- Power BI dataflows
- SQL Server
- Analysis Services
- Text/CSV
- Web
- OData feed
- Blank query

More... Write a query from scratch.

Advanced Editor

Open the Advanced Query Editing dialog to view or modify the entire text for this query.

Query1

Query1

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

# STEPS

Advanced Editor

## Query1

Display Options ?

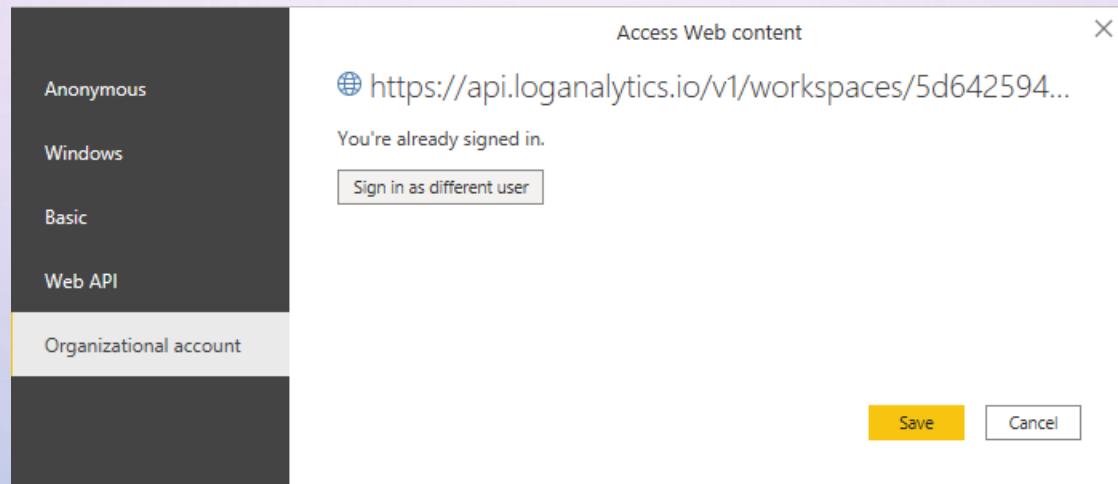
```
1  /*
2  The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel
3  and Power BI Desktop.
4  For Power BI Desktop follow the instructions below:
5  1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/
6  2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'
7  3) Paste the M Language script into the Advanced Query Editor and select 'Done'
8 */
9
10
11 let AnalyticsQuery =
12 let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/5d6425-...2d/query",
13 [Query=[#"query"="AuditAzureActiveDirectory_CL
14 ",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="P1D",#"prefer"="ai.response-thinning=true"],Timeout=#duration(0,0,4,0)])),
15 TypeMap = #table(
16 { "AnalyticsTypes", "Type" },
17 {
18 { "string", Text.Type },
19 { "int", Int32.Type },
20 { "long", Int64.Type },
21 { "real", Double.Type },
22 { "timespan", Duration.Type },
23 { "datetime", DateTimeZone.Type },
24 { "bool", Logical.Type },
25 { "guid", Text.Type },
26 { "dynamic", Text.Type }
27 }),
28 DataTable = Source[tables]{0},
29 Columns = Table.FromRecords(DataTable[columns]),
30 ColumnsWithType = Table.Join(Columns, { "type" }, TypeMap , {"AnalyticsTypes"}),
31 Rows = Table.FromRows(DataTable[rows], Columns[name]),
32 Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3} } ))
33 in
34 Table
35 in AnalyticsQuery
```

✓ No syntax errors have been detected.

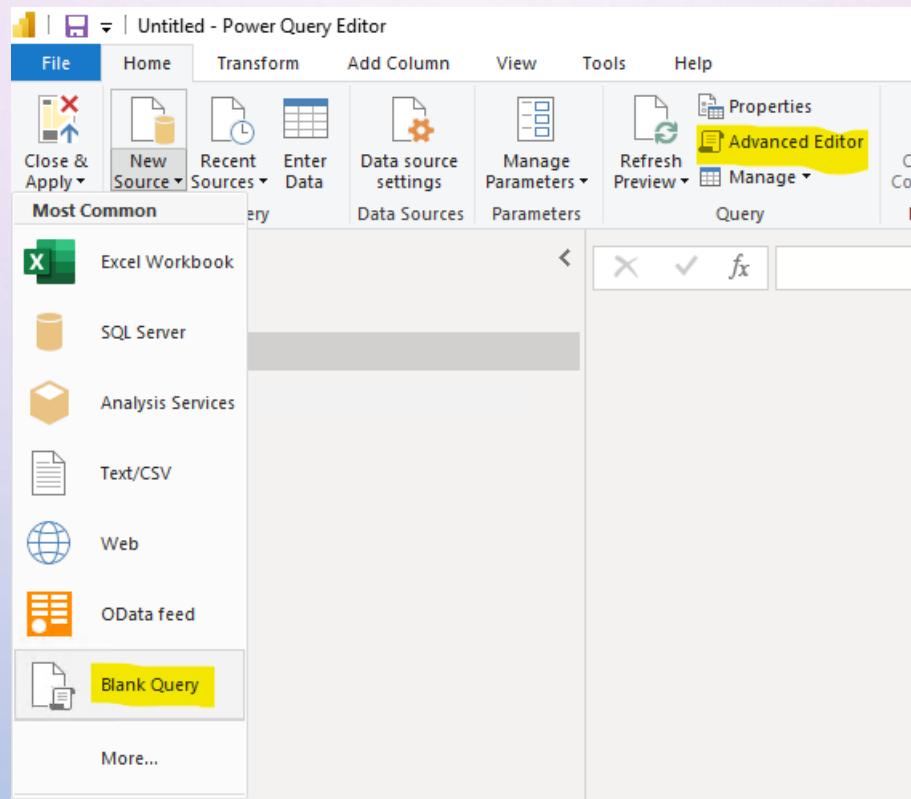
Done Cancel



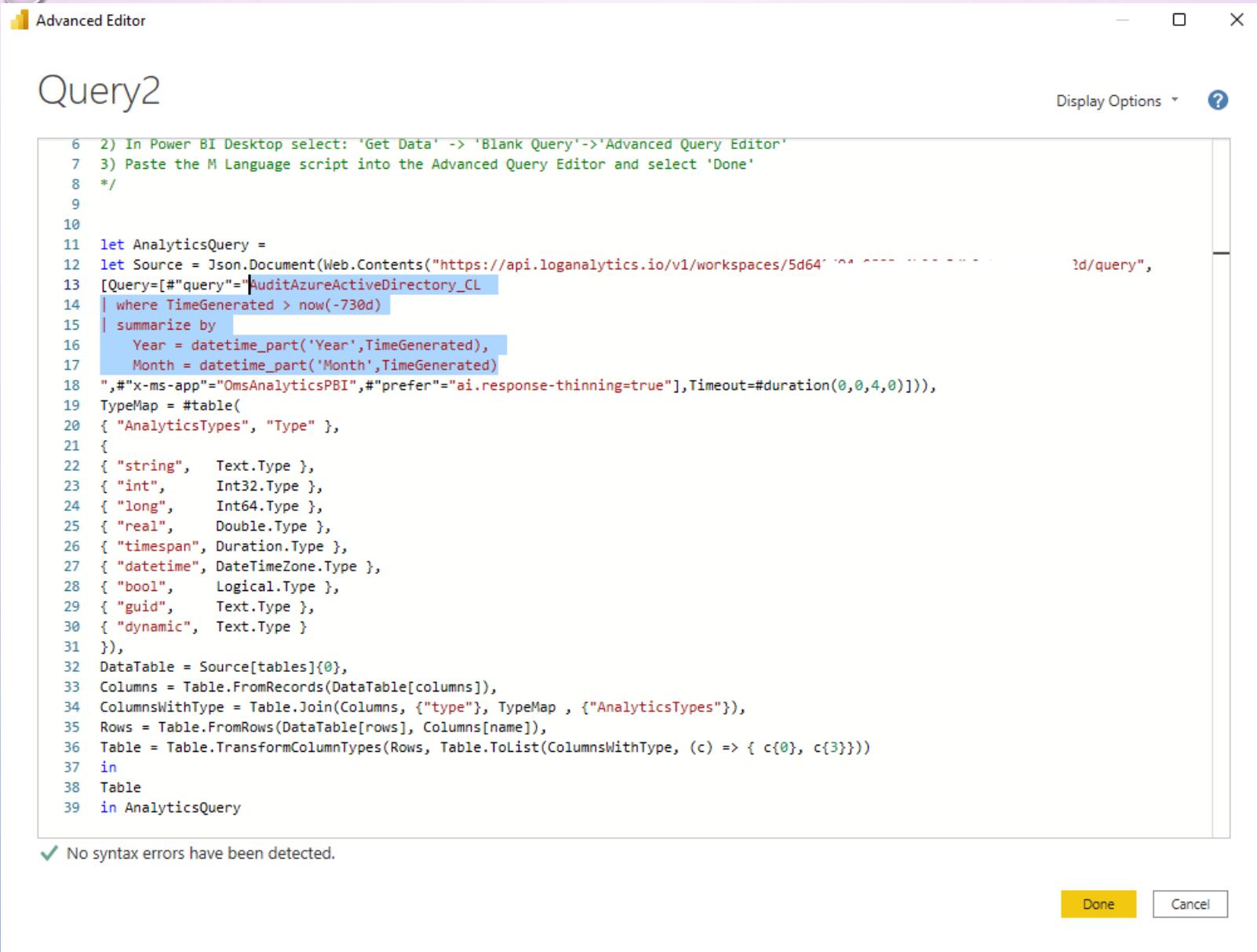
## STEPS



# STEPS



# STEPS



# STEPS

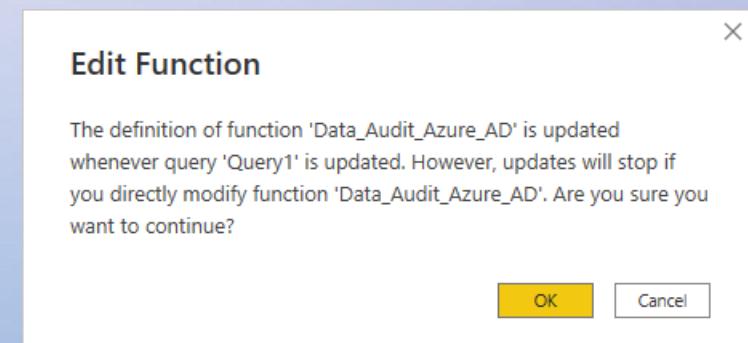
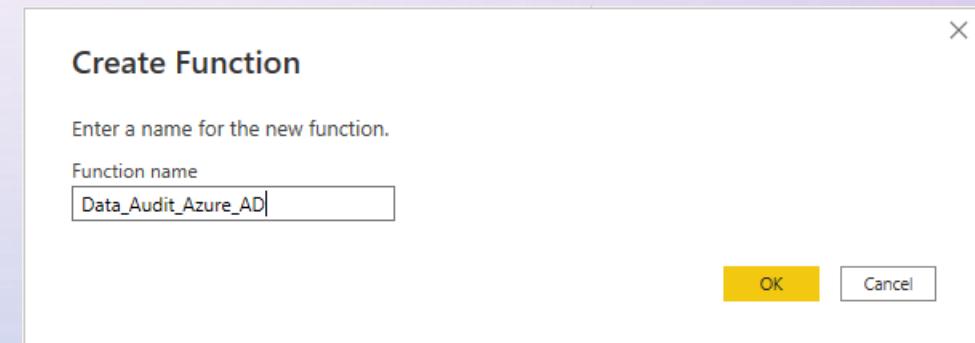
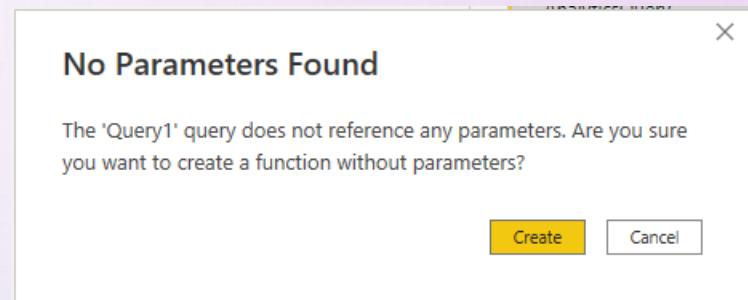
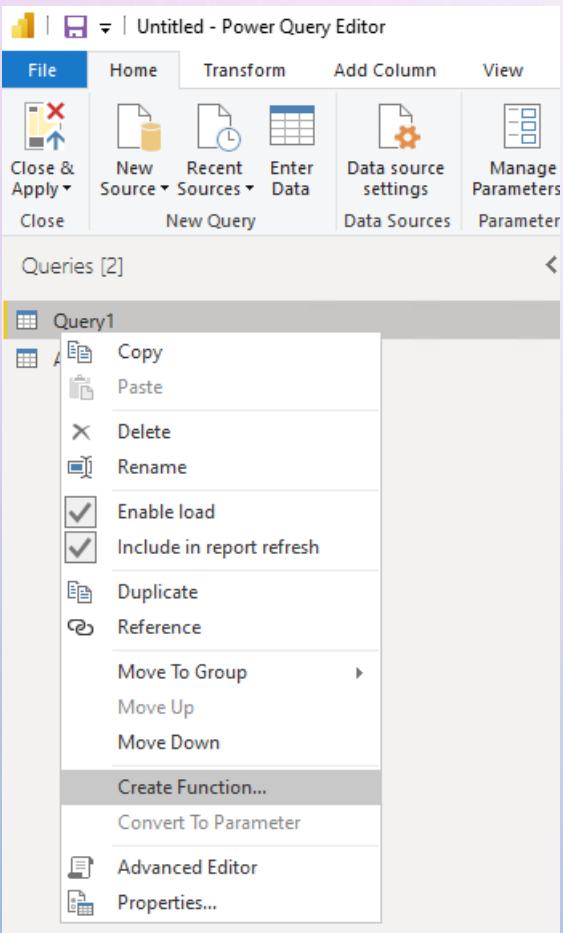
The screenshot shows the Microsoft Power Query Editor interface. The title bar reads "Untitled - Power Query Editor". The ribbon menu is visible with tabs like File, Home, Transform, Add Column, View, Tools, and Help. The Home tab is selected.

The main area displays a query titled "Query1" which has been loaded from a JSON document. The formula bar shows the M code: `= let Source = Json.Document(Web.Contents("https://"))`. Below the formula bar, there is a preview pane showing a table with three columns: "Year" (containing "123"), "Month" (containing "123"), and "2022" (containing the value "8").

The "Transform" tab is active, showing various tools for managing columns, rows, and data types. A "Sort" section is visible, and the "Data Type" dropdown is set to "Whole Number".

On the right side, the "Query Settings" pane is open, showing the "Properties" section where the "Name" is set to "Audit Azure Active Directory". The "Applied Steps" section lists a single step named "AnalyticsQuery".

## STEPS



## STEPS

Advanced Editor

### Data\_Audit\_Azure\_AD

Display Options ?

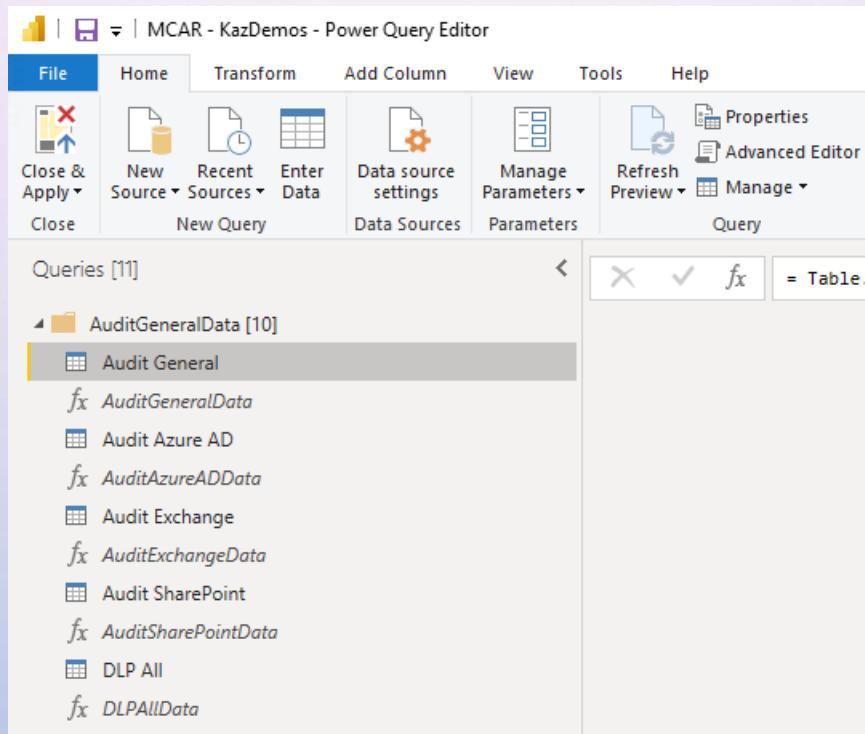
```
1 let
2   Source = (Month as text, Year as text) => let AnalyticsQuery =
3     let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/5d642d/query",
4       [Query="#query=""AuditAzureActiveDirectory_CL
5       ",#x-ms-app="OmsAnalyticsPBI",#timespan="AuditAzureActiveDirectory_CL | where datetime_part('Month',TimeGenerated) == "& Month &" and datetime_part('Year'
6       TypeMap = #table(
7         { "AnalyticsTypes", "Type" },
8         {
9           { "string", Text.Type },
10          { "int", Int32.Type },
11          { "long", Int64.Type },
12          { "real", Double.Type },
13          { "timespan", Duration.Type },
14          { "datetime", DateTimeZone.Type },
15          { "bool", Logical.Type },
16          { "guid", Text.Type },
17          { "dynamic", Text.Type }
18        )),
19        DataTable = Source[tables]{0},
20        Columns = Table.FromRecords(DataTable[columns]),
21        ColumnsWithType = Table.Join(Columns, {"type"}, TypeMap , {"AnalyticsTypes"}),
22        Rows = Table.FromRows(DataTable[rows], Columns[name]),
23        Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3}}))
24      in
25      Table
26      in AnalyticsQuery
```

✓ No syntax errors have been detected.

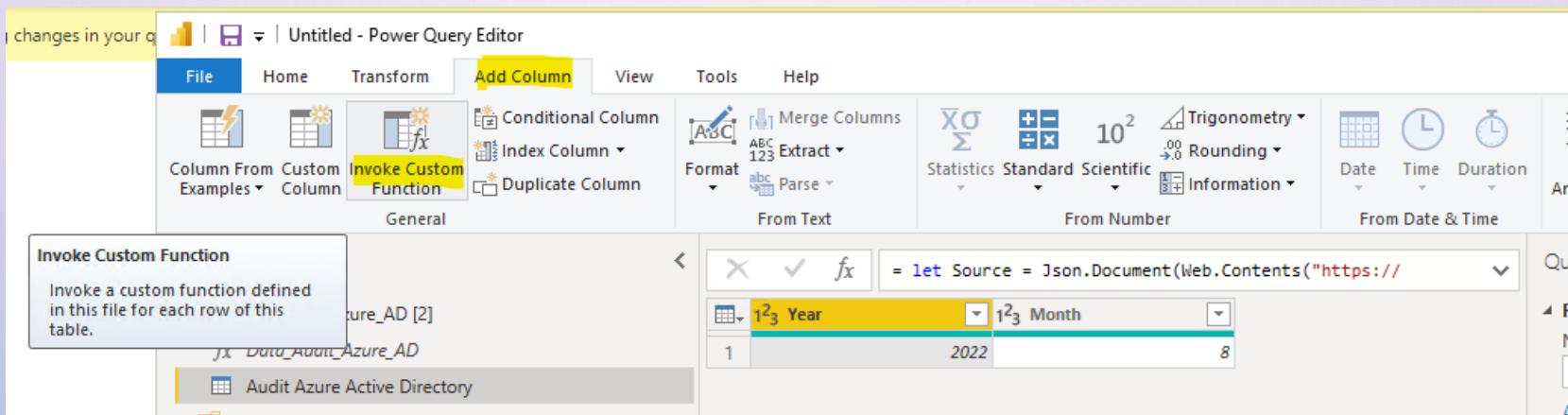
Done Cancel



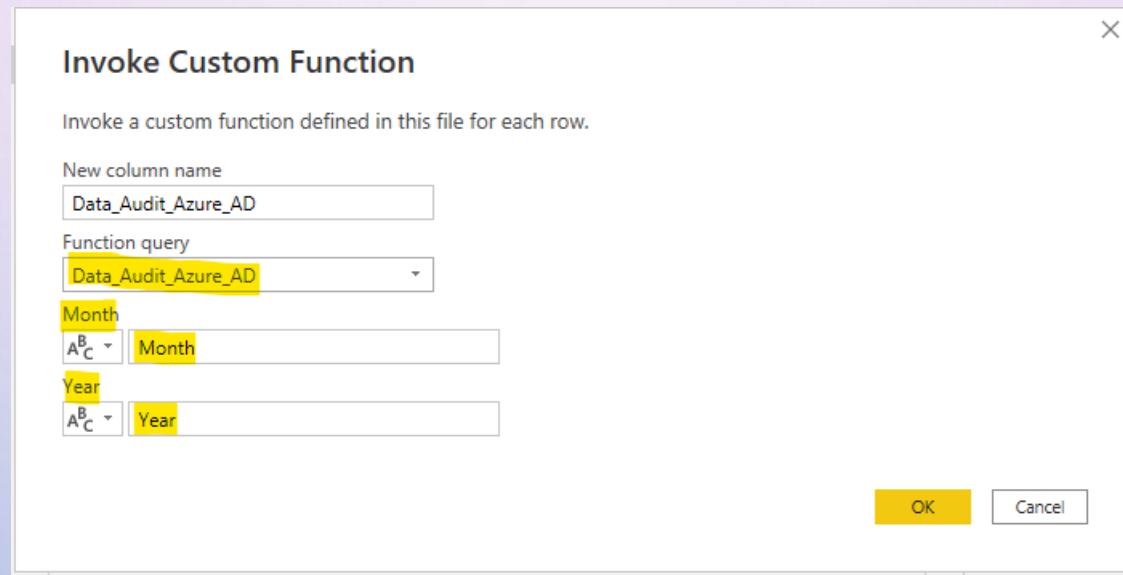
# STEPS



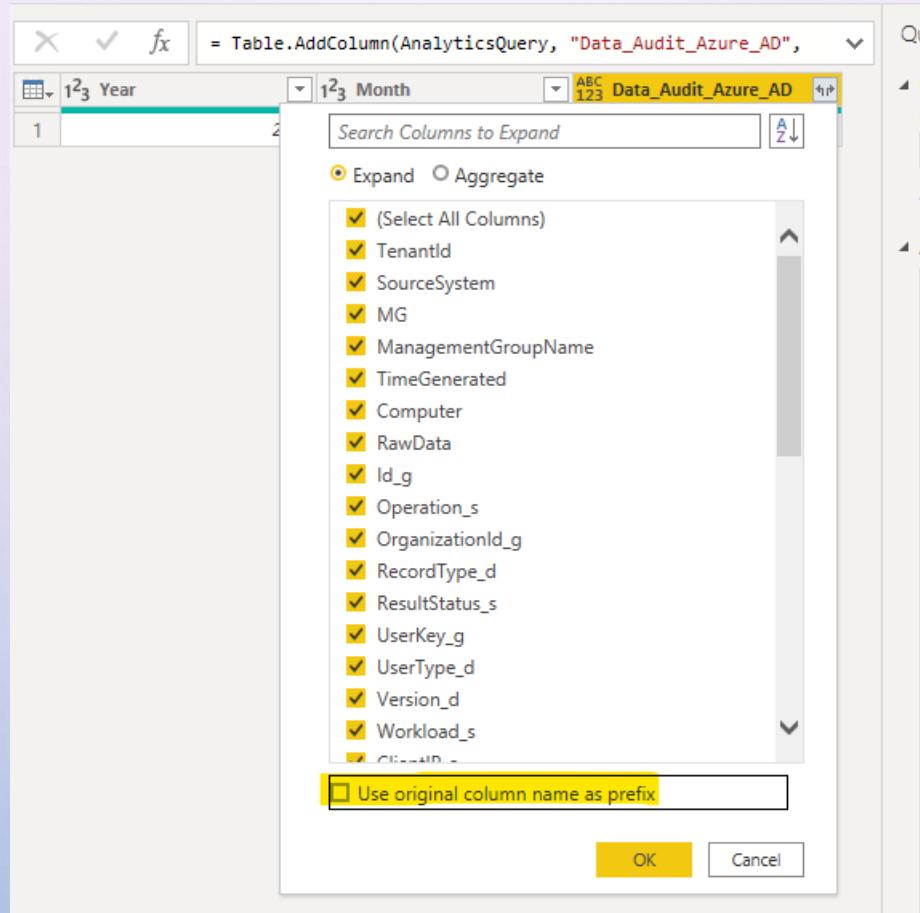
# STEPS



## STEPS



# STEPS

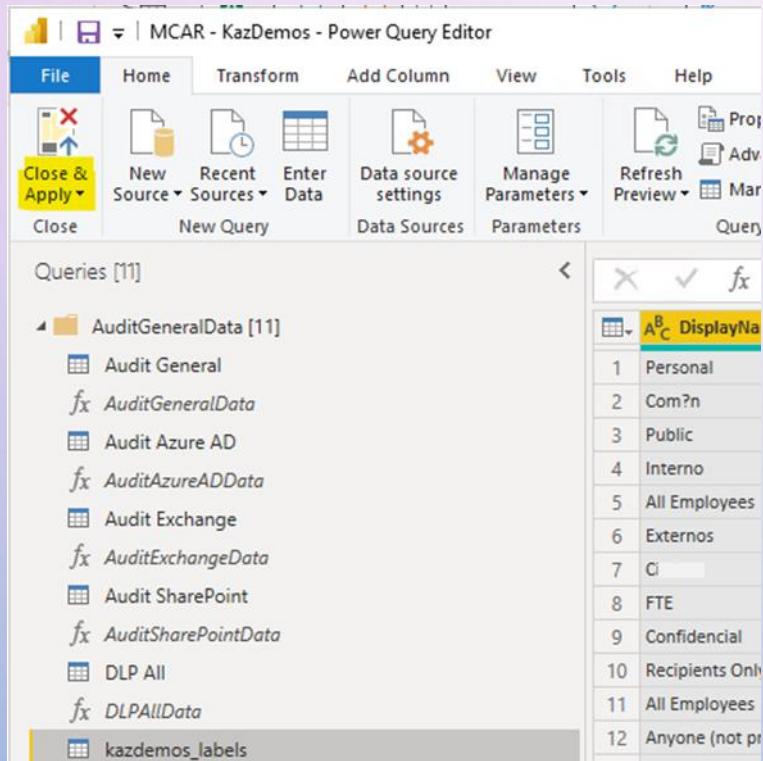


# STEPS

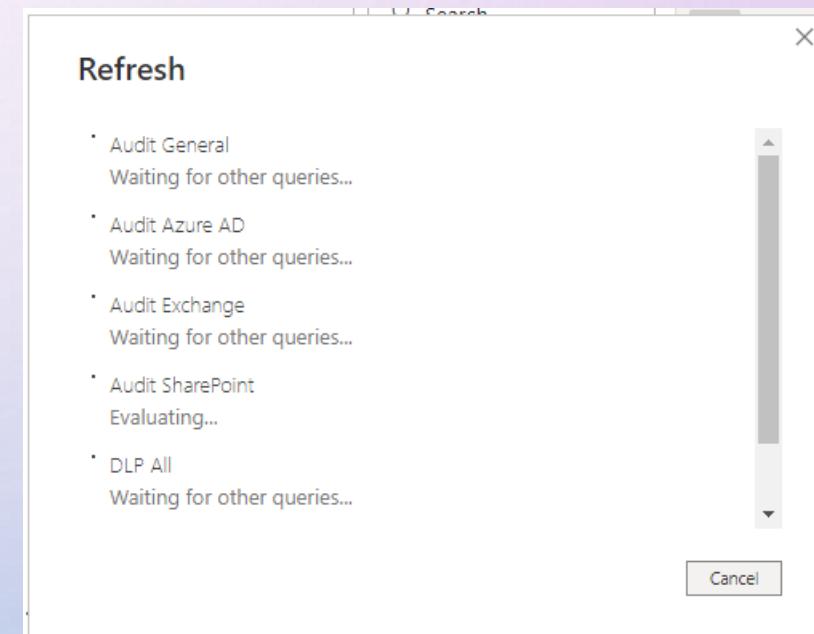
The screenshot shows the Microsoft Power BI Data Editor interface. The 'Home' tab is selected in the ribbon. On the left, the 'Queries [2]' pane shows two queries: 'Data\_Audit\_Azure\_AD [2]' and 'Audit Azure Active Directory'. The 'Audit Azure Active Directory' query is currently selected. The main area displays a table with three rows of data. The first column contains row numbers (1, 2, 3). The second column is labeled 'ManagementGroupNa...' and contains three empty cells. The third column is labeled 'TimeGenerated' and contains three timestamp values: '8/20/2022 7:45:23 AM +00:00', '8/20/2022 7:45:23 AM +00:00', and '8/20/2022 10:56:27 AM +00:00'. A context menu is open over the 'TimeGenerated' column, specifically over the third row. The 'Data Type' dropdown menu is visible, with 'Date/Time/Timezone' selected. Other options in the dropdown include 'Decimal Number', 'Fixed decimal number', 'Whole Number', 'Percentage', 'Date/Time', 'Date', 'Time', 'Duration', 'Text', 'True/False', and 'Binary'.

	ManagementGroupNa...	TimeGenerated
1		8/20/2022 7:45:23 AM +00:00
2		8/20/2022 7:45:23 AM +00:00
3		8/20/2022 10:56:27 AM +00:00

# STEPS



The screenshot shows the Power Query Editor interface with the title bar "MCAR - KazDemos - Power Query Editor". The ribbon menu includes File, Home, Transform, Add Column, View, Tools, and Help. The Home tab is selected. The toolbar contains icons for Close, New Source, Recent Sources, Enter Data, Data source settings, Manage Parameters, Refresh, Preview, and Close & Apply. The "Close & Apply" button is highlighted with a yellow box. The main area displays a list of queries under the heading "Queries [11]". One query, "AuditGeneralData [11]", is expanded, showing its sub-queries: Audit General, Audit Azure AD, Audit Exchange, Audit SharePoint, and DLP All. At the bottom of the list is "kazdemos\_labels". A small preview pane on the right shows a table with columns "DisplayNa" and "Value", containing items like Personal, Com?n, Public, Interno, All Employees, Externos, Ci, FTE, Confidencial, Recipients Only, All Employees, and Anyone (not pr).



The screenshot shows a "Refresh" dialog box with the title "Refresh". It lists several queries and their current status: Audit General (Waiting for other queries...), Audit Azure AD (Waiting for other queries...), Audit Exchange (Waiting for other queries...), Audit SharePoint (Evaluating...), and DLP All (Waiting for other queries...). A "Cancel" button is visible at the bottom right.

# STEPS

The screenshot shows the Power BI Desktop interface with the following details:

- Home Tab:** Selected tab.
- Data:** Get data from various sources like Excel, Data, SQL Server, and Dataverse.
- Queries:** Transform and refresh data.
- Insert:** New visual, Text box, More visuals.
- Calculations:** New measure, Quick measure, Sensitivity.
- Sensitivity:** Publish.

**Pie Chart:** Visual titled "Count of UserId\_s by UserId\_s". The chart is divided into 10 equal segments, each labeled "1 (10%)". The legend lists "Userid\_s" with corresponding colors and names:

- Certificate
- firm\_password\_service@support.on...
- mike.wazowski@kazdemos.org
- Not Available
- randall.boggs@kazdemos.org
- sebastian.zamorano.adm@kazdemos...
- ServicePrincipal 1b4d105e-6b01-4a...
- ServicePrincipal 4eceacb2-6c0a-478...
- ServicePrincipal 697b1d8d-1c87-4a...
- ServicePrincipal ed05063e-6d20-44...

**Visualizations pane:** Shows the current visualization selected: "Audit Exchange". Other items listed include "Audit General", "Audit SharePoint", "DLP All", and "kazdemos\_labels".

**Fields pane:** Displays available fields for selection.

**Page navigation:** Shows "Page 1" of 1.

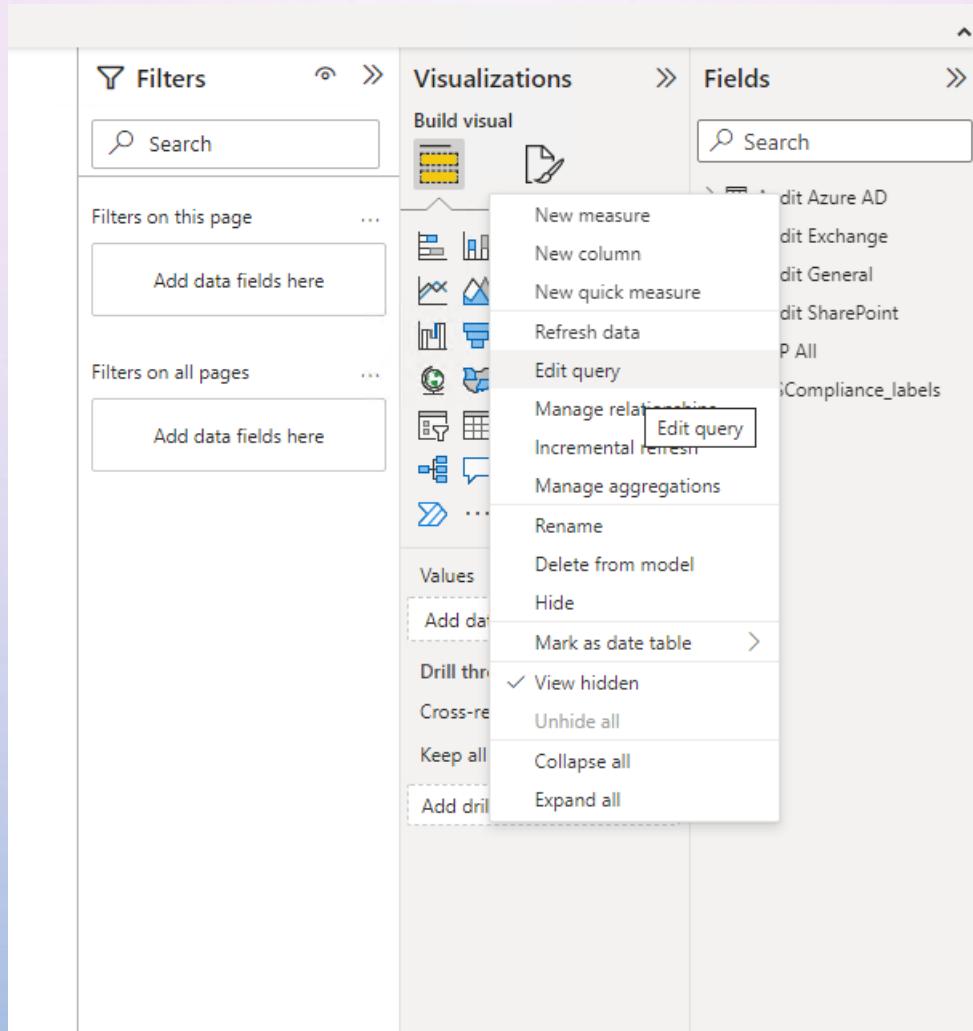
## TO SIMPLIFY, WE CAN CREATE TEMPLATES

- TO EASILY EXPORT OUR POWER BI EFFORT, DO THE NEXT STEPS:
  1. RIGHT CLICK AT LEFT OVER ANY OF THE TABLE NAMES AND SELECT EDIT QUERY
  2. UNDER POWER QUERY EDITOR GO TO MANAGE PARAMETERS AND SELECT NEW PARAMETER
  3. ON THE NEW POP-UP WINDOW ADD THESE:
    - NAME: **WORKSPACE\_ID**
    - DESCRIPTION: WORKSPACE ID FROM LOGS ANALYTICS
    - CHECK REQUIRED
    - TYPE: TEXT
    - SUGGESTED VALUES: ANY VALUE
    - CURRENT VALUE: *{ADD YOUR WORKSPACE ID FROM LOGS ANALYTICS}*
  4. AFTER THAT, IN EACH TABLE(5) AND FUNCTION(5) IS REQUIRED CHANGE THE WORKSPACE ID WITH THE NEW VARIABLE GO THROUGH ADVANCED EDITOR

```
LET SOURCE = JSON.DOCUMENT(WEB.CONTENT("HTTPS://API.LOGANALYTICS.IO/V1/WORKSPACES/" & WORKSPACE_ID  
& "/QUERY",
```

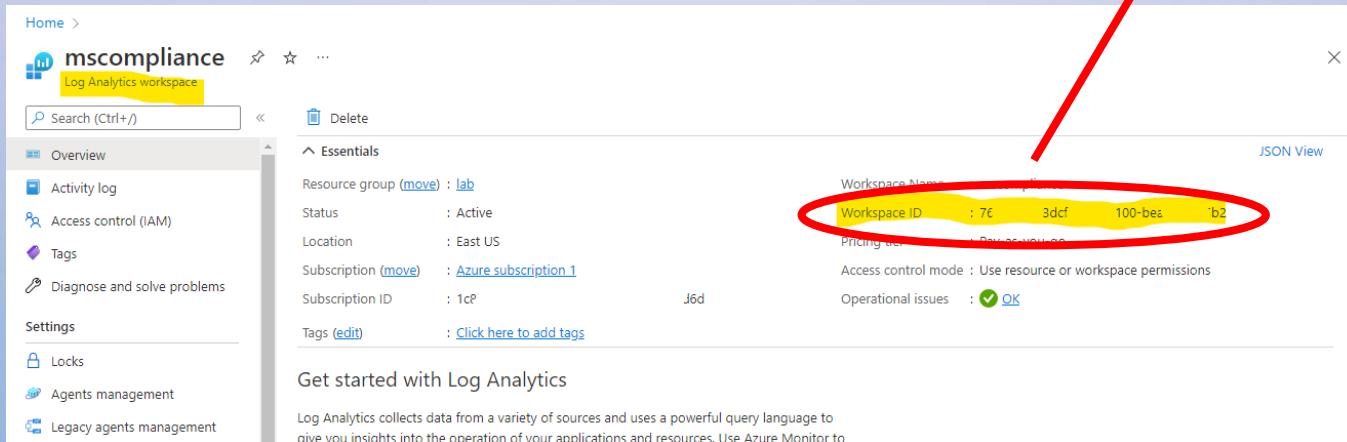
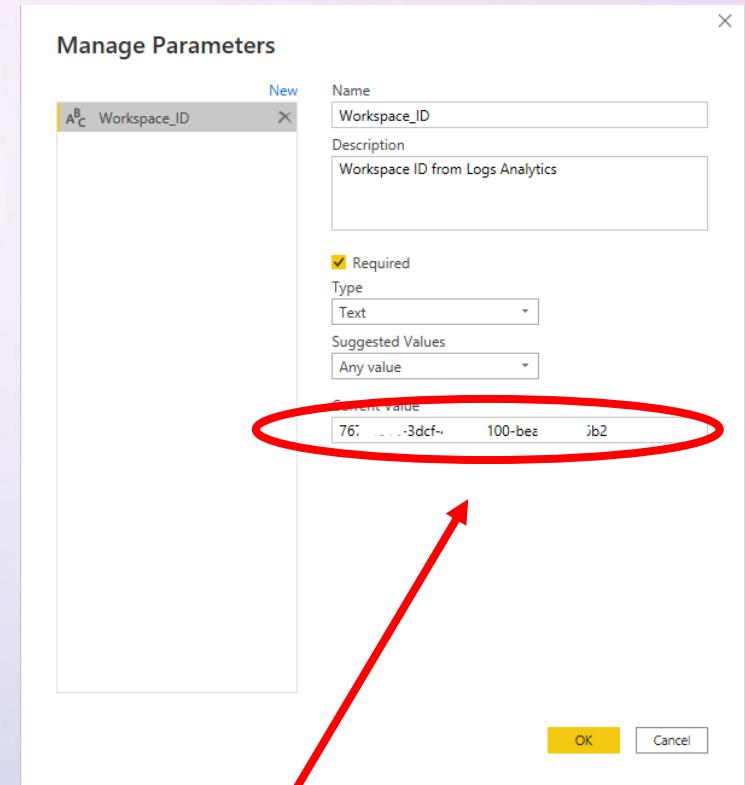
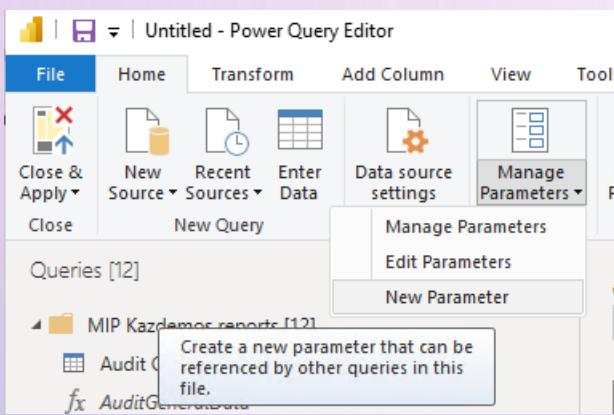
5. AFTER FINISH, PRESS CLOSE & APPLY
6. TO EXPORT GO TO FILE AND SELECT EXPORT AND SELECT POWER BI TEMPLATE
7. ADD A TEMPLATE DESCRIPTION
8. SET A FILE NAME AND LOCATION AND SAVE

## STEPS



# POWER BI - TEMPLATES

## STEPS



## STEPS

The screenshot shows the Microsoft Power Query Editor interface. The title bar reads "Untitled - Power Query Editor". The ribbon menu includes File, Home, Transform, Add Column, View, Tools, and Help. The Home tab is selected. The ribbon also features Close & Apply, New, Recent, Sources, Data, Advanced Editor, Properties, Merge Queries, Append Queries, and Use First Row as Headers.

The left pane displays a tree view of "Queries [12]" under "MIP Kazdemos reports [12]". The "Audit General" query is selected, highlighted with a yellow border. Other queries listed include Audit GeneralData, Audit Azure AD, Audit Exchange, Audit SharePoint, DLP All, MSCompliance\_labels, and Workspace\_ID (76781014-3dc).

The main workspace is titled "Audit General". It contains the following M Language script:

```
1 /*  
2 The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel  
3 and Power BI Desktop.  
4 For Power BI Desktop follow the instructions below:  
5 1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/  
6 2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'  
7 3) Paste the M Language script into the Advanced Query Editor and select 'Done'  
8 */  
9  
10  
11 let AnalyticsQuery =  
12 let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/" & Workspace_ID & "/query",  
13 [Query="#query=AuditGeneral_CL  
14 | where TimeGenerated > now(-730d)  
15 | summarize by  
16 Year = datetime_part('Year',TimeGenerated),  
17 Month = datetime_part('Month',TimeGenerated)  
18 ",#"x-ms-app="OmsAnalyticsPBI",#"prefer="ai.response-thinning=true"],Timeout=#duration(0,0,4,0)])),  
19 TypeMap = #table(  
20 { "AnalyticsTypes", "Type" },  
21 {  
22 { "string", Text.Type },  
23 { "int", Int32.Type },  
24 { "long", Int64.Type },  
25 { "real", Double.Type },  
26 { "timespan", Duration.Type },
```

A green checkmark icon and the text "No syntax errors have been detected." are displayed at the bottom left of the code area. At the bottom right are "Done" and "Cancel" buttons.

## STEPS

The screenshot shows the Microsoft Power Query Editor interface. The title bar reads "Untitled - Power Query Editor". The ribbon menu includes File, Home, Transform, Add Column, View, Tools, and Help. The Home tab is selected. The ribbon also features Close & Apply, New, Recent, Sources, Data, Properties, Advanced Editor, and various data transformation icons like Sort, Filter, and Pivot.

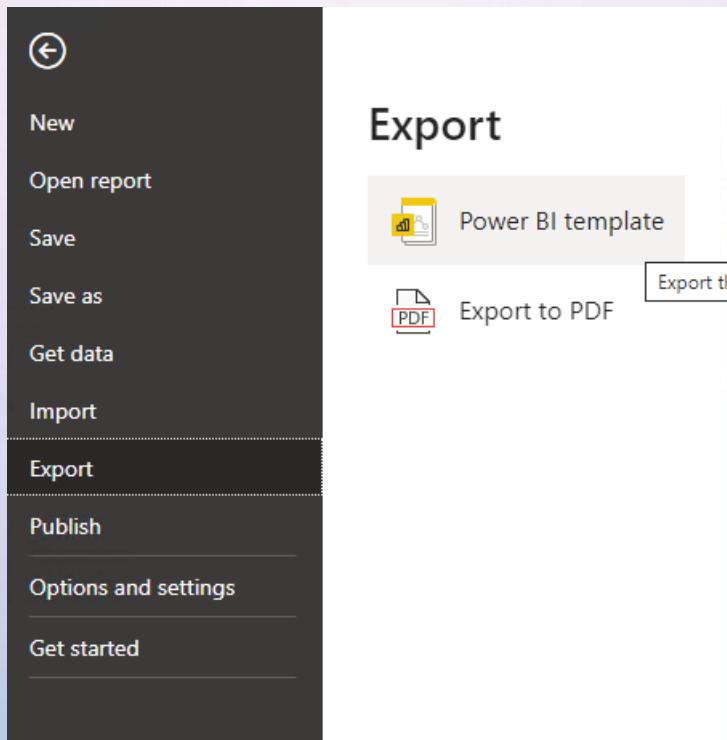
The left pane displays the "Queries [12]" list. Under the "MIP Kazdemos reports [12]" folder, the "Audit General" folder is expanded, showing the "AuditGeneralData" query. Other queries listed include Audit Azure AD, AuditAzureADData, Audit Exchange, AuditExchangeData, Audit SharePoint, AuditSharePointData, DLP All, DLPAllData, MSCompliance\_Labels, and Workspace\_ID (76781014-3dc). The "Other Queries" folder is also present.

The main workspace is titled "AuditGeneralData". It contains the MPPNQ code for the query:

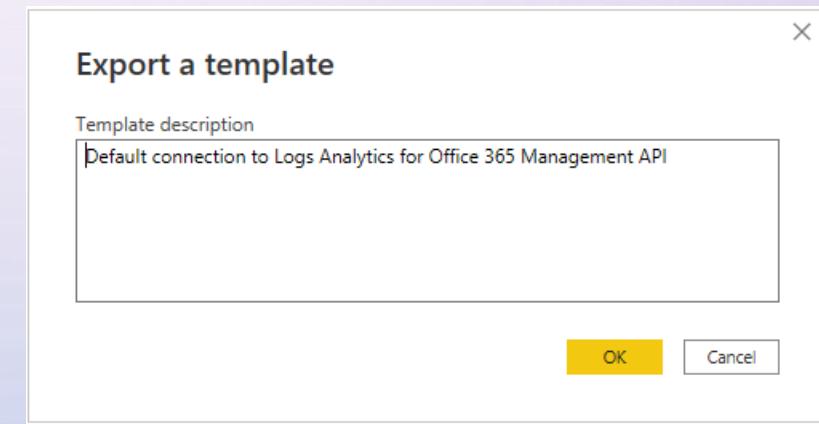
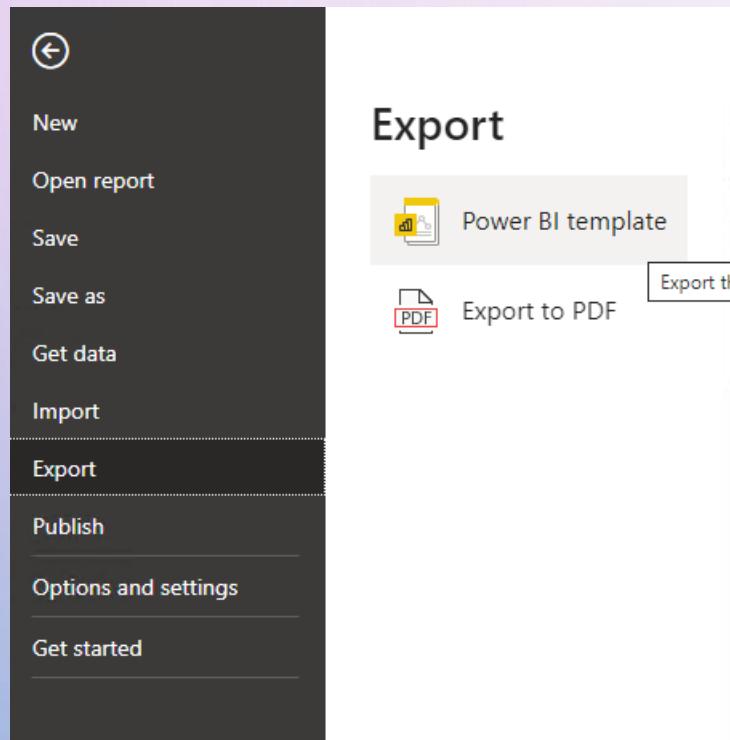
```
1 let
2     Source = (Month as text, Year as text) => let AnalyticsQuery =
3         let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/& Workspace_ID &/query",
4             [Query=#"query"="AuditGeneral_CL
5             ,#"x-ms-app"="OmsAnalyticsPBI","#timespan"="AuditGeneral_CL | where datetime_part('Month',TimeGenerated) == "& Month &" and datetime_
6             TypeMap = #table(
7                 { "AnalyticsTypes", "Type" },
8                 [
9                     { "string", Text.Type },
10                    { "int", Int32.Type },
11                    { "long", Int64.Type },
12                    { "real", Double.Type },
13                    { "timespan", Duration.Type },
14                    { "datetime", DateTimeZone.Type },
15                    { "bool", Logical.Type },
16                    { "guid", Text.Type },
17                    { "dynamic", Text.Type }
18                }),
19                DataTable = Source[tables]{0},
20                Columns = Table.FromRecords(DataTable[columns]),
21                ColumnsWithType = Table.Join(Columns, {"type"}, TypeMap, {"AnalyticsTypes"}),
22                Rows = Table.FromRows(DataTable[rows], Columns[name]),
23                Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3}}))
24            in
25            Table
26            in AnalyticsQuery
```

A green checkmark icon and the text "No syntax errors have been detected." are displayed at the bottom of the code area. At the bottom right are "Done" and "Cancel" buttons.

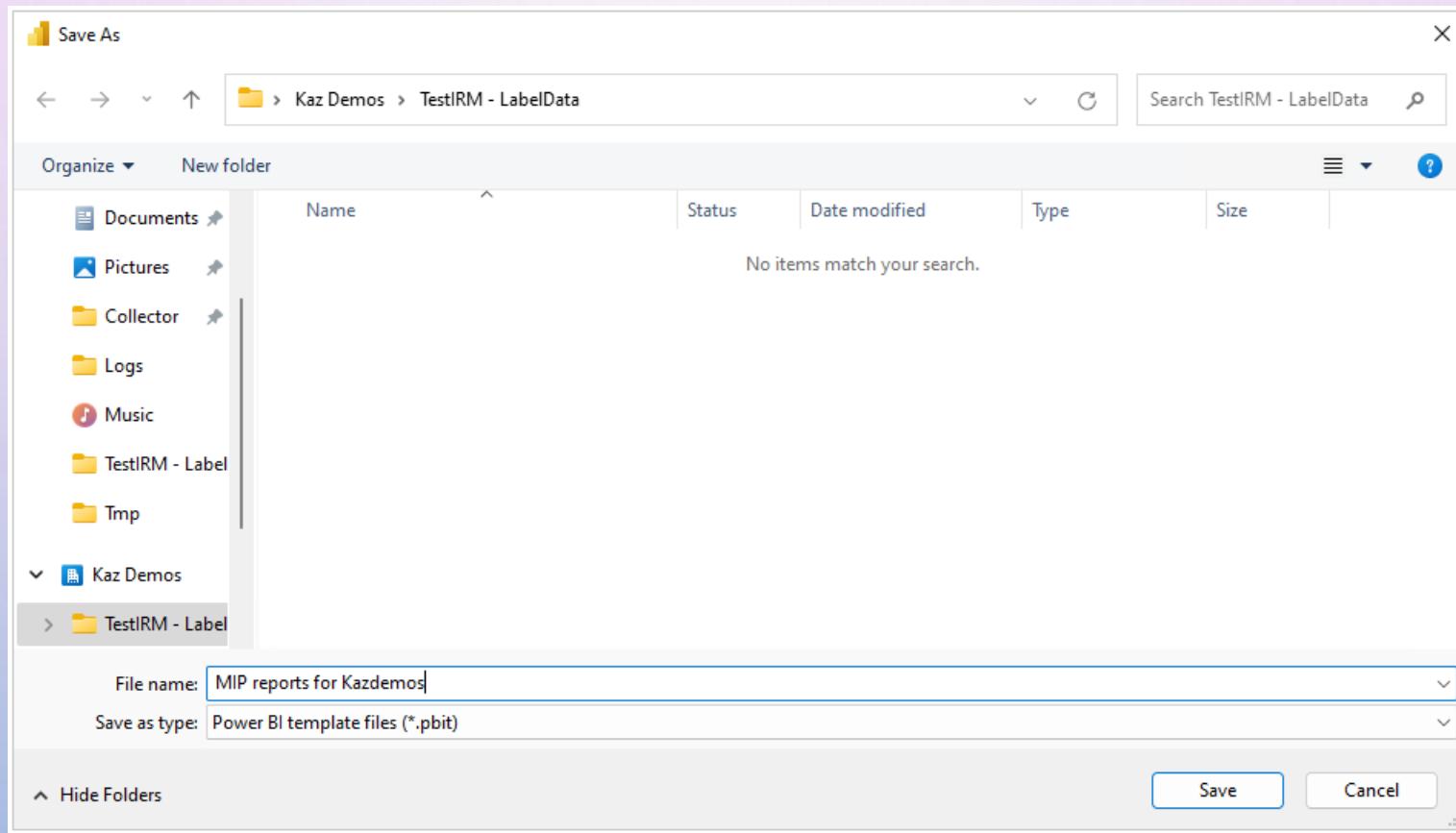
## STEPS



## STEPS

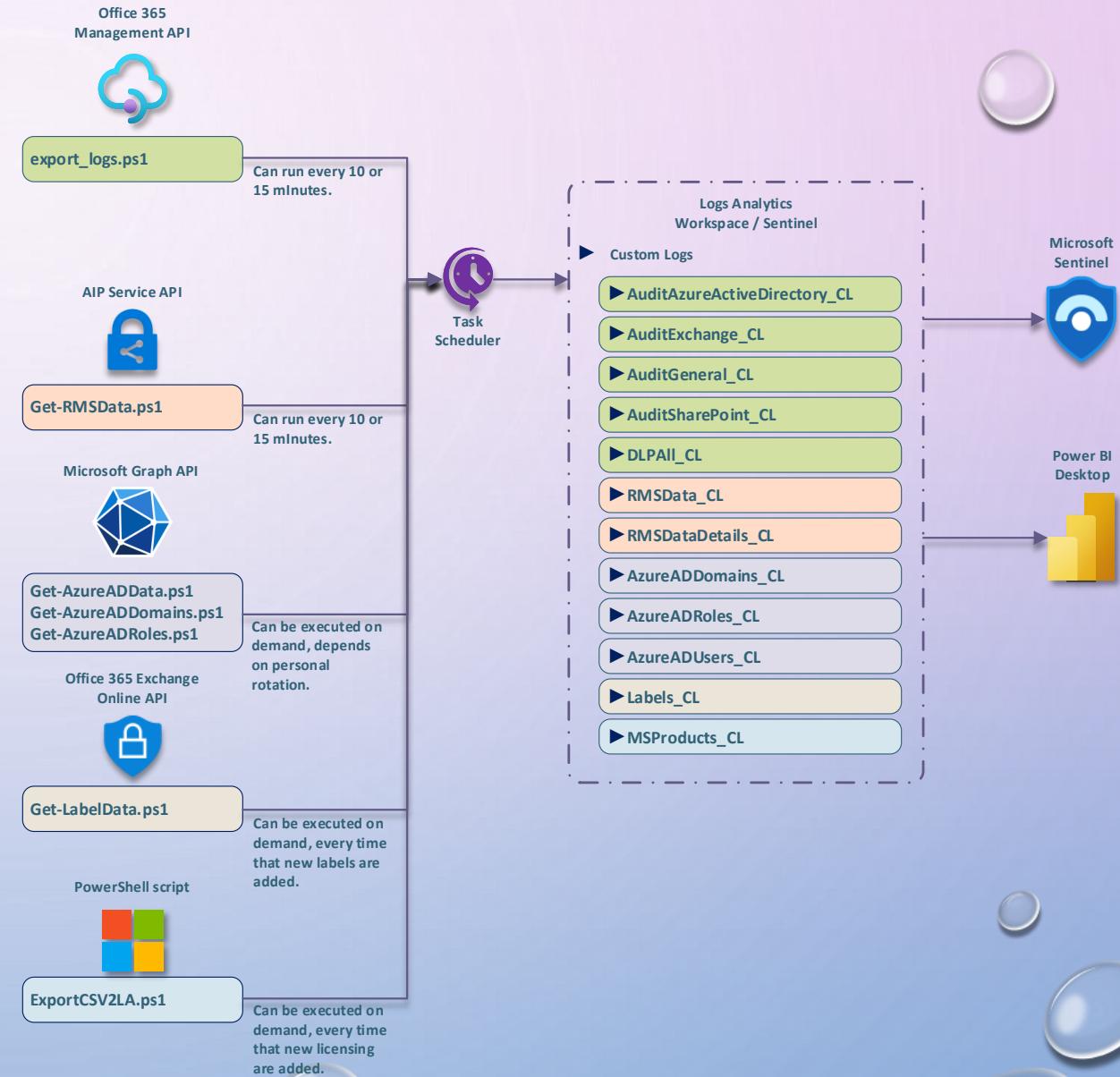


# STEPS



## TO IMPORT ADVANCED POWER BI TEMPLATE

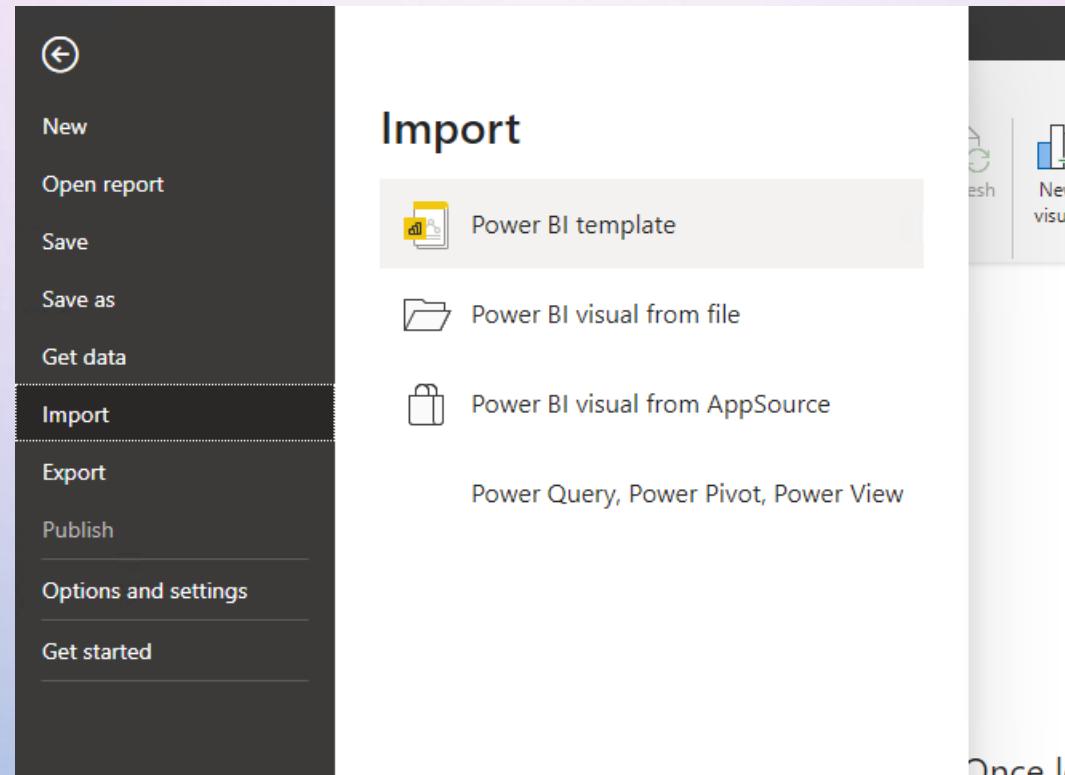
- VALIDATE THESE SCRIPTS WAS EXECUTED FIRST:
  - EXPORT\_LOGS.PS1 AND IS RUNNING UNDER TASK SCHEDULER
  - .\EXPORTCSV2LA.PS1 -FILENAME '\SUPPORT DATA\PRODUCT NAMES AND SERVICE PLAN IDENTIFIERS FOR LICENSING.CSV' -TABLENAME MSPRODUCTS (WAS EXECUTED AND THE TABLENAME IS CREATED WITH THE SAME NAME SHOWN)
  - .\GET-AZUREADDATA.PS1 (RUN ON DEMAND)
  - .\GET-AZUREADROLES.PS1 (RUN ON DEMAND)
  - .\GET-AZUREADDOMAINS.PS1 (RUN ON DEMAND)
  - .\GET-LABELDATA.PS1 (RUN ON DEMAND)
  - .\GET-RMSDATA.PS1 AND IS RUNNING UNDER TASK SCHEDULER
- IF IT'S THE FIRST TIME WAIT AROUND 15 MINUTES UNTIL THE TABLES ARE POPULATED AND APPEAR UNDER CUSTOM LOGS ON LOGS MENU IN YOUR LOGS ANALYTICS WORKSPACE



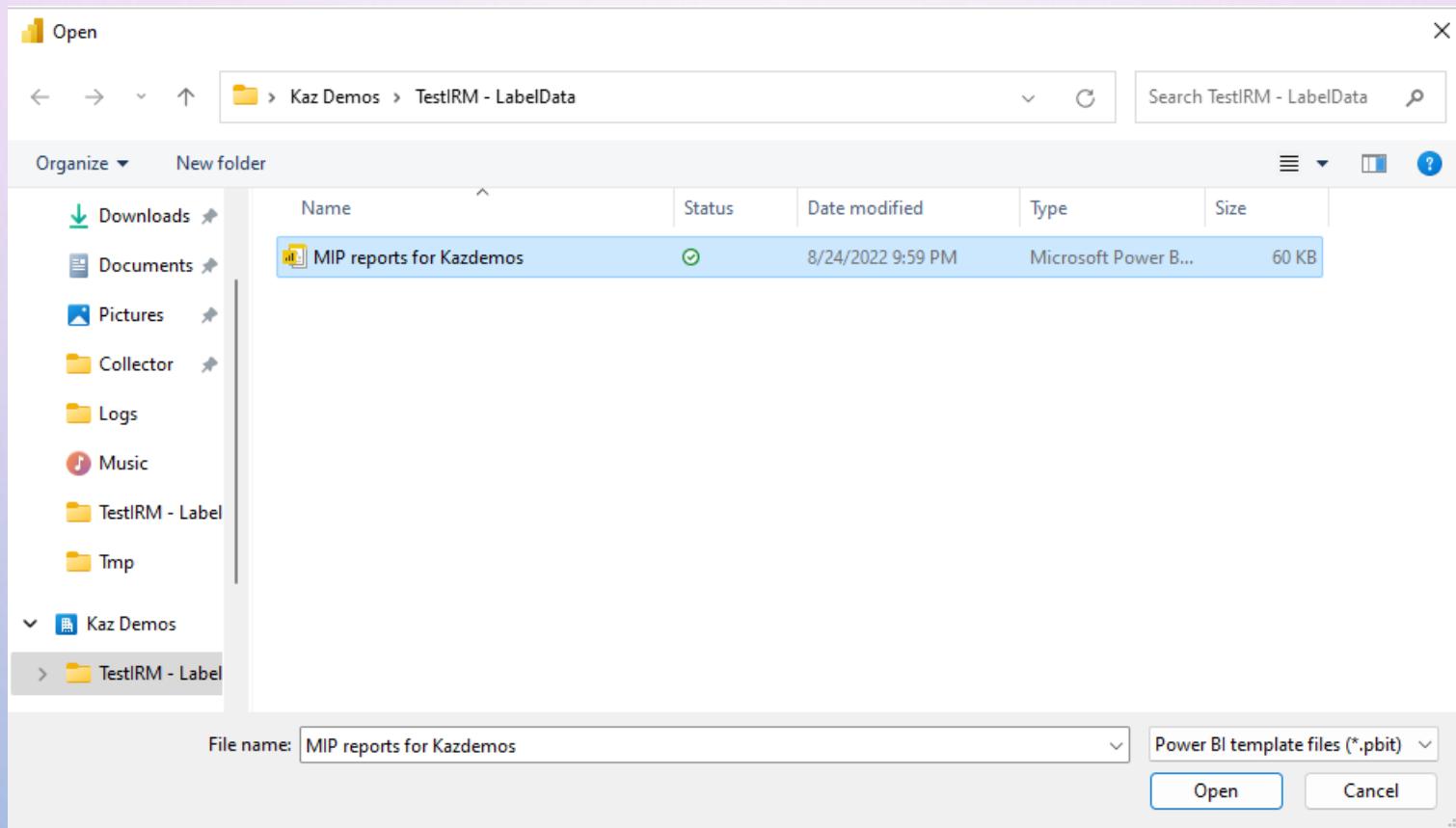
## TO IMPORT A TEMPLATE

- WITH THIS STEPS WE WILL REDUCE A LOT THE PREVIOUS EFFORT TO CONNECT EACH DATA SOURCE AND ALL THE PREVIOUS CONFIGURATION
- OPEN POWER BI DESKTOP
- CLOSE THE POP-UP WINDOW
- GO TO FILE THEN IMPORT AND SELECT POWER BI TEMPLATE
- LOCATE YOUR TEMPLATE FILE, SELECT THEM AND PRESS OPEN
- WORKSPACE\_ID WILL BE REQUIRED, ENTER YOUR WORKSPACE ID AND PRESS LOAD
- DEPENDING THE ACCOUNT USED AS SIGN-IN ON POWER BI, NEW CREDENTIALS WILL BE REQUIRED
- TO VALIDATE THE RIGHT SETTINGS, OPEN POWER QUERY EDITOR DOING A RIGHT CLICK OVER ANY OF THE TABLE NAMES LOCATED AT LEFT UNDER FIELDS AND SELECTING EDIT QUERY
- CHECK WORKSPACE\_ID VARIABLE THAT MATCH WITH YOUR WORKSPACE ID
- VALIDATE THAT YOU ARE USING THE RIGHT MATRIX FOR LABEL NAMES AND GUIDS, IN CASE THAT NOT MATCH WITH THE CURRENT WORKSPACE ID INFORMATION, REMOVE AND CREATE A NEW ONE BASED ON PREVIOUS STEPS EXPLANATION.
- CLOSE & APPLY

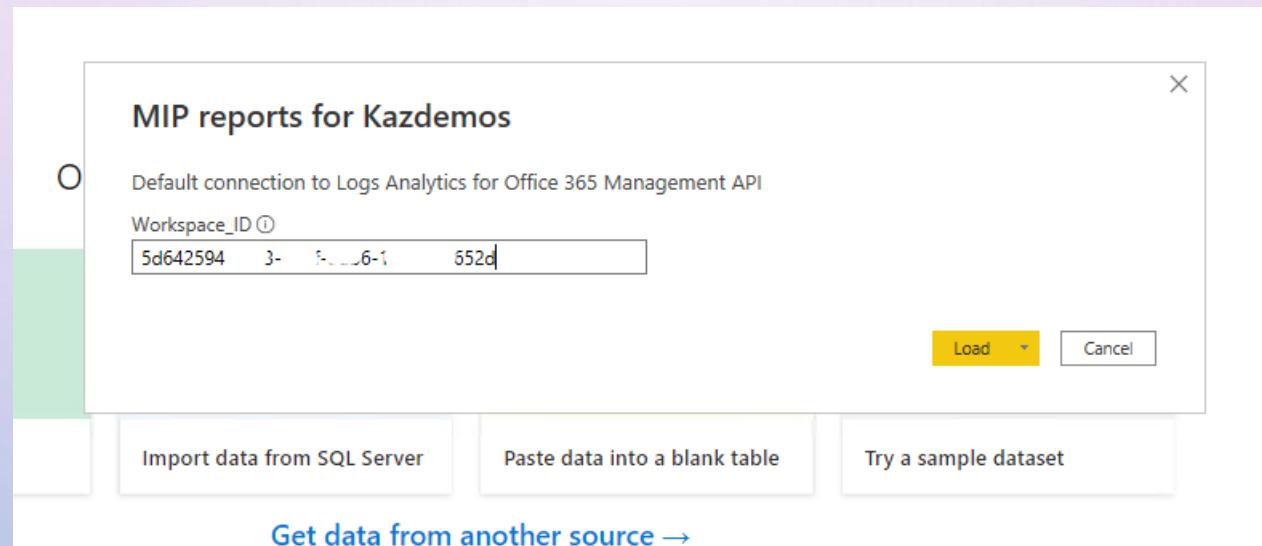
## STEPS



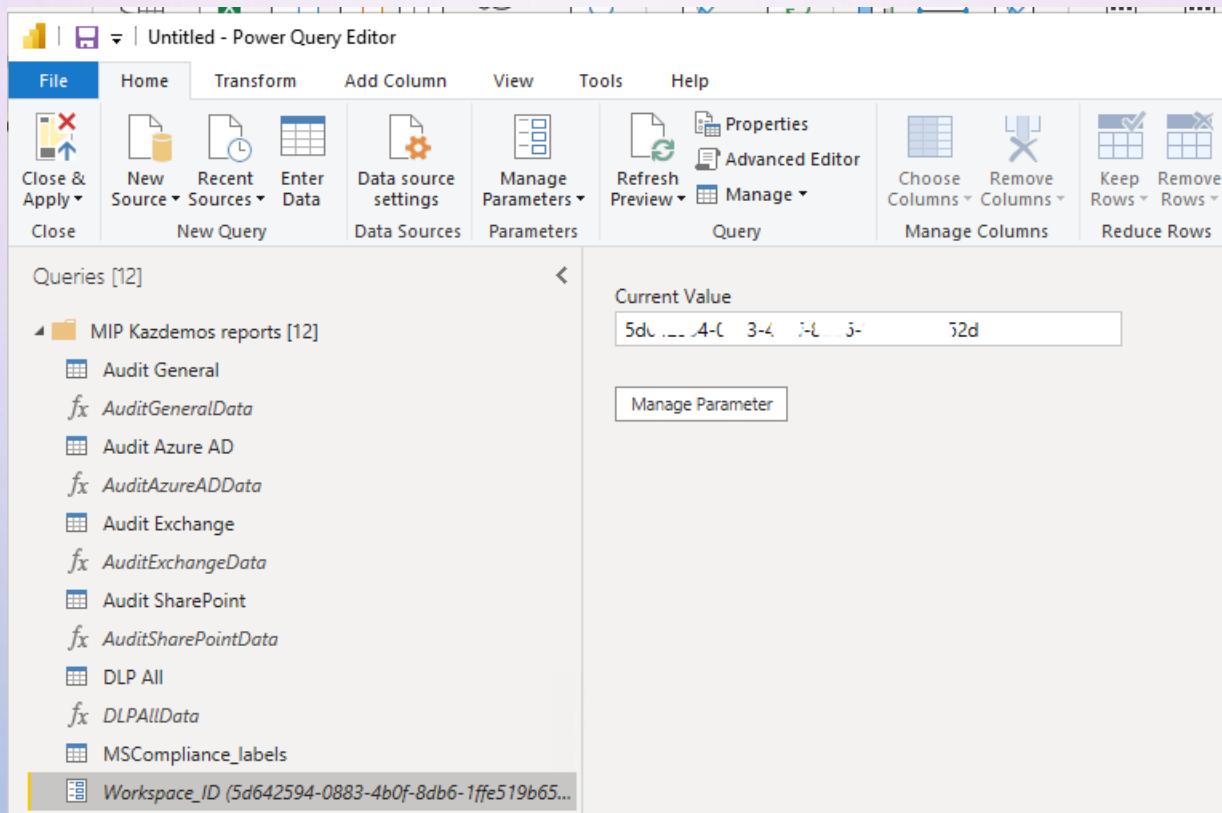
## STEPS



## STEPS



## STEPS



## TO CREATE A FUNCTION ON POWER BI FOR GEO LOCATION BASED ON IP ADDRESSES

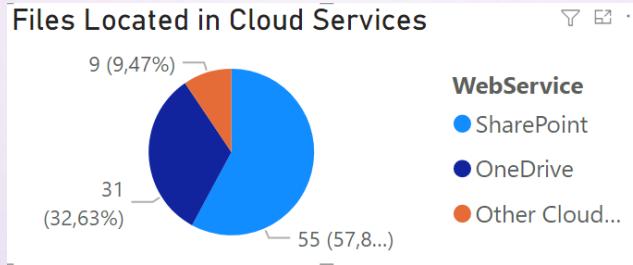
- OPEN POWER BI, PRESS “GET DATA” AND SELECT “BLANK QUERY” IN THE NEW WINDOW OPEN SELECT “ADVANCED EDITOR” AND REPLACE THE CONTENT WITH THIS FUNCTION.

```
LET  
    SOURCE = (#"IP ADDRESS" AS TEXT) => LET  
        SOURCE = JSON.DOCUMENT(WEB.CONTENTS("HTTP://IPWHOIS.APP/JSON/" & #"IP ADDRESS")),  
        #"CONVERTED TO TABLE" = RECORD.TOTABLE(SOURCE),  
        #"TRANSPOSED TABLE" = TABLE.TRANSPOSE(#"CONVERTED TO TABLE"),  
        #"PROMOTED HEADERS" = TABLE.PROMOTEHEADERS(#"TRANSPOSED TABLE")  
    IN  
    #"PROMOTED HEADERS"  
    IN  
    SOURCE
```

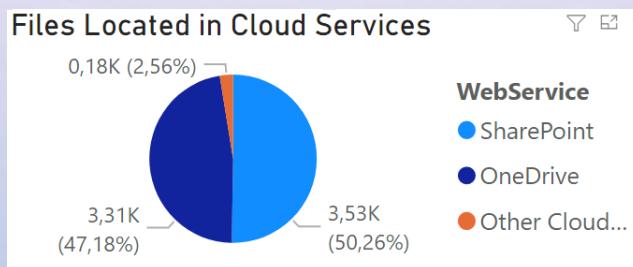
- AT LEFT MENU CHANGE THE NAME TO SOMETHING LIKE AS “GEOLOCATIONFUNCTION”

## AVOID SOME BAD REPORTS

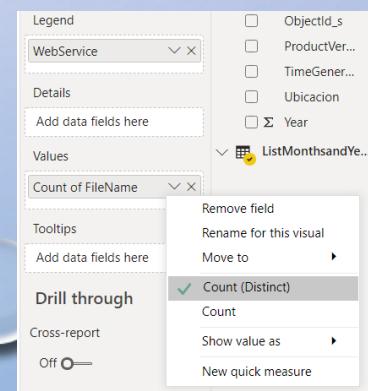
- SOMETIMES WE NEED TAKE CARE WITH THE VALUES AND FILTERS USED WHEN WE CREATE OUR REPORTS TO SHOW WRONG INFORMATION, HERE AN EXAMPLE:



- IN THE IMAGE SHOWN WE ADD A FILTER TO COUNT DISTINCT FILENAME, BUT THE LEGEND IS RELATED TO FILES LOCATED IN CLOUD SERVICES, IF WE CAN NOT DO THAT, WE OBTAIN THIS RESULT:



- YOU CAN MAKE THE CHANGE IN THE SAME POWER BI ON FILTERS



## LINKS OF INTEREST

- [INCREMENTAL REFRESH IN POWER BI](#)
- [SENSITIVITY LABELS IN POWER BI](#)
- [EXCEED THE 500,000 ROW LIMIT IN APPLICATION INSIGHTS AND LOG ANALYTICS WITH POWER BI](#)
- [KUSTO](#)

### ##### URL USED #####

- [POWER BI QUERY EDITOR - GETTING IP ADDRESS DETAILS FROM IP ADDRESS - REPORTING/ANALYTICS MADE EASY WITH FOURMOO AND POWER BI](#)

### ##### GEO LOCATION SERVICES BY IP #####

- [14 BEST IP GEOLOCATION API TO OFFER PERSONALIZED CONTENT \(GEEKFLARE.COM\)](#)

### ##### GEO LOCATION APIs TESTED #####

- [IP LOOKUP API AND IP GEOLOCATION DOCUMENTATION \(IPWHOIS.IO\)](#)
- [IP-API.COM - GEOLOCATION API - DOCUMENTATION - JSON \(IP-API.COM\)](#)
- [PRICING | IP GEOLOCATION API \(IPIFY.ORG\)](#)
- [IP GEOLOCATION API WITH COUNTRY INFORMATION](#)
- [FREE IP GEOLOCATION API AND ACCURATE IP GEOLOCATION DATABASE](#)



# THANK YOU

SEBASTIÁN ZAMORANO



+56 9 5207 3058



SEBASTIAN.ZAMORANO@MICROSOFT.COM



WWW.MICROSOFT.COM



myprofile.kazblog.me



<https://aka.ms/bingthrivekudos>

## SOME ADDITIONAL EFFORT TO RELEASE SOON

- II KUSTO QUERIES FOR THE NEW SCHEMA, THE IDEA IS DOWNLOAD ONLY COLUMNS REQUIRED FOR THIS REPORTS
- ✓ SOME EXAMPLES AND TEMPLATES FOR POWER BI DASHBOARDS
- ✓ GEO LOCATION ON POWER BI BASED ON IP ADDRESS
- ✓ ADD AZURE AD SCHEMA TO GENERATE REPORTS BASED ON AREAS OR DEPARTMENTS
- ✓ ADD AZURE RMS LOGS TO SHOW ACCESS FROM EXTERNAL USERS TO PROTECTED INFORMATION
- II INCREMENTAL REFRESH ON POWER BI TO REDUCE LOGS ANALYTICS COST
- ✓ PUBLISH DIFFERENT REPORTS FOR SEPARATE AUDIENCE ON POWER BI ONLINE
- II FIELDS DICTIONARY
- II RELATIONSHIP MAP BETWEEN TABLES