Microsoft

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)

GitHub

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 B.I 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?

AGENDA

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

Microsoft

DASHBOARDS

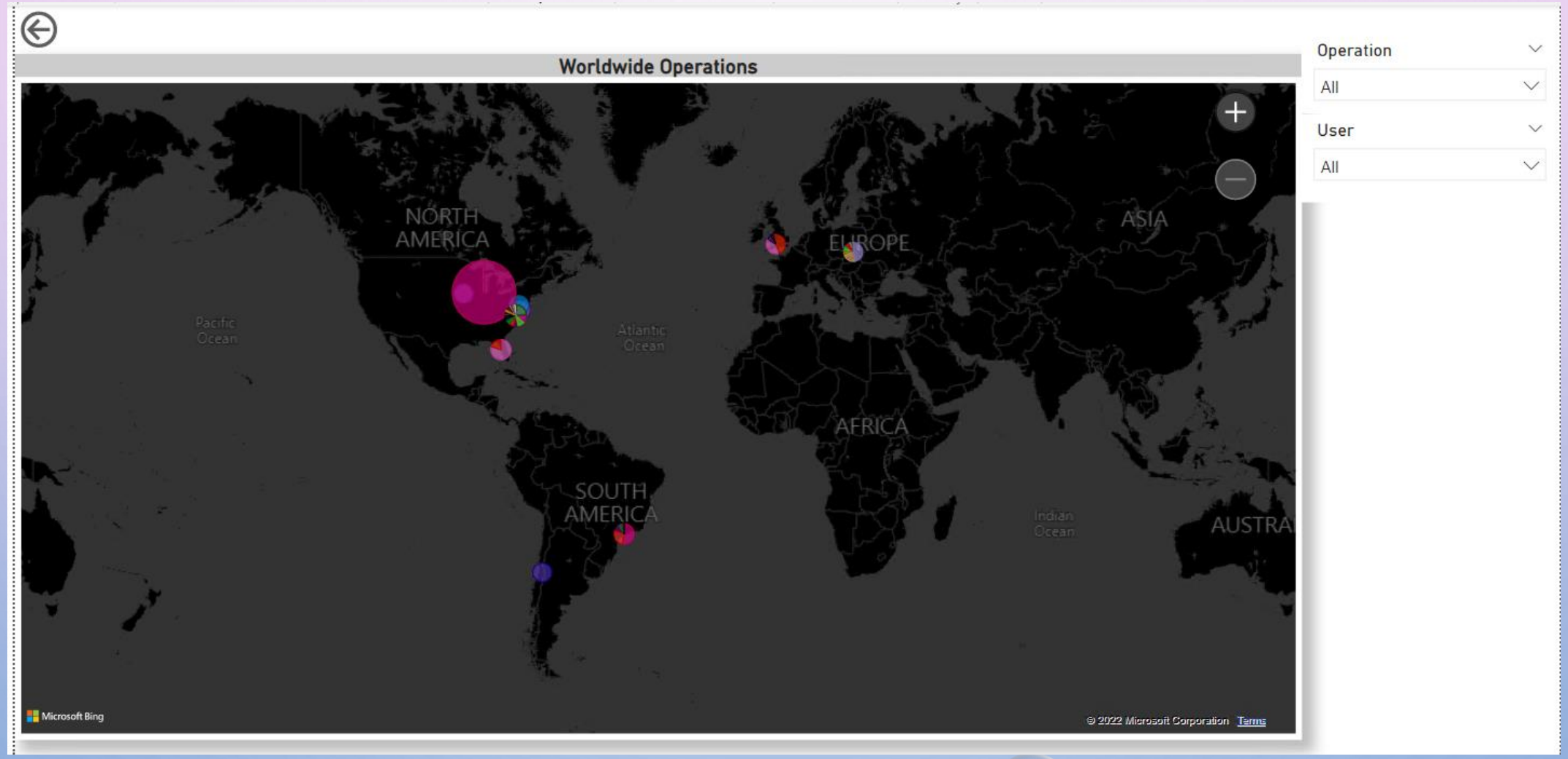
SOME SAMPLE REPORTS

DASHBOARD - OVERVIEW

DASHBOARD FOR UNIFIED LABELING BEHAVIOR

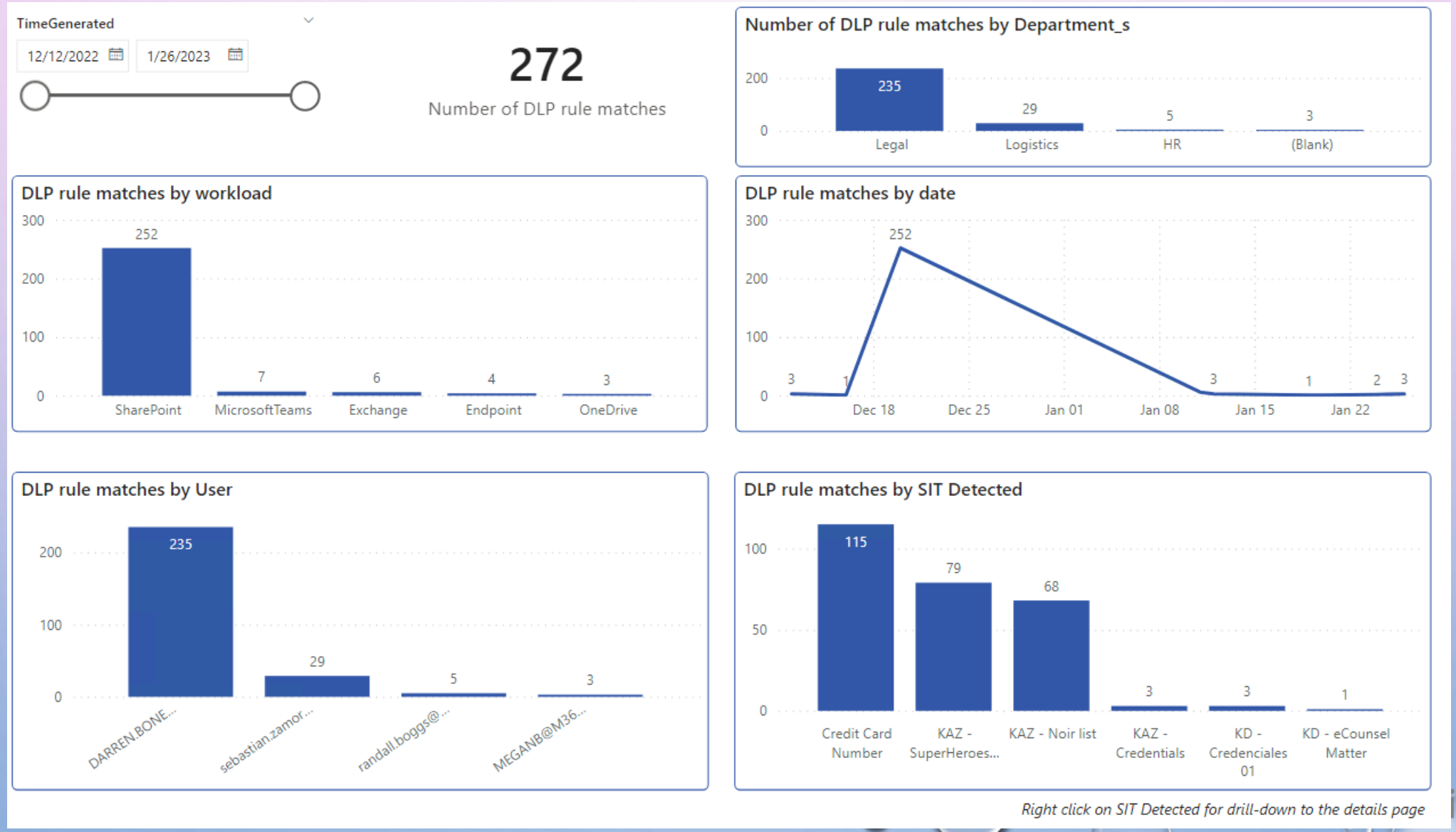
DASHBOARD – GEO LOCATION

DASHBOARD FOR AUDIT ACTIVITIES



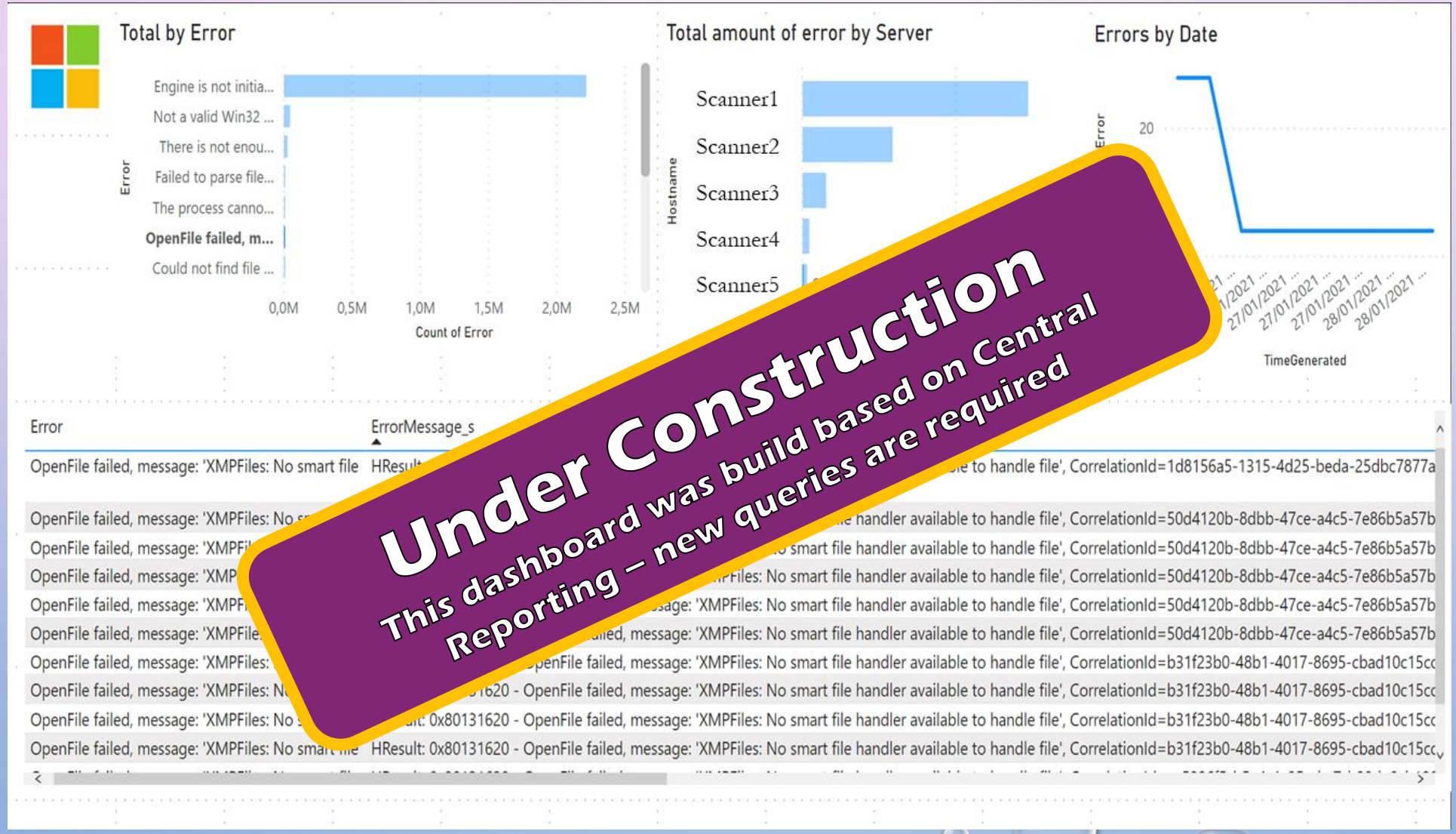
DASHBOARD – USER BEHAVIOR

DASHBOARD FOR DLP ACTIVITIES



DASHBOARD – AIP SCANNER

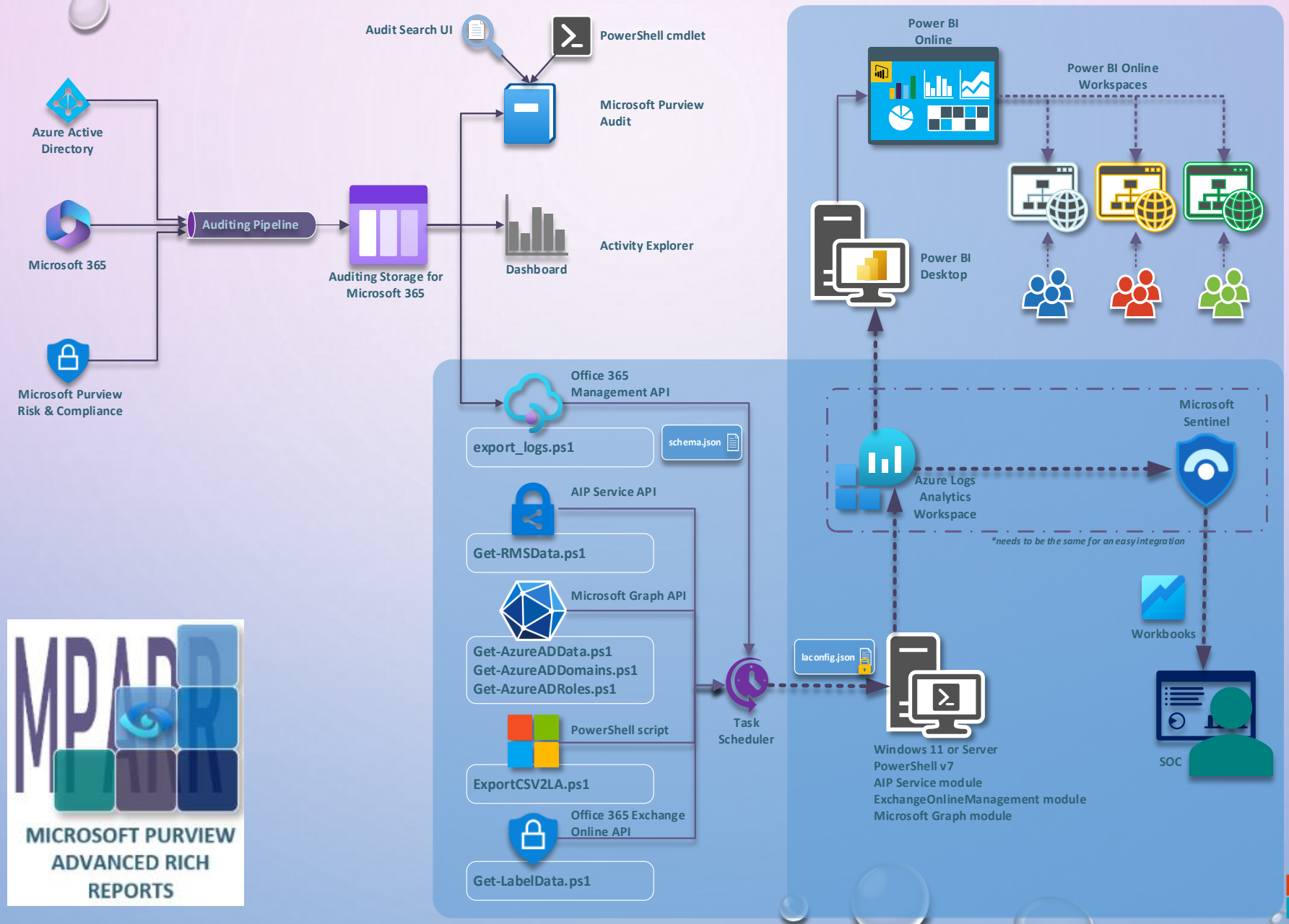
DASHBOARD FOR AUDIT ACTIVITIES



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 PURVIEW ADVANCED RICH REPORTS

CHECKLIST

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**

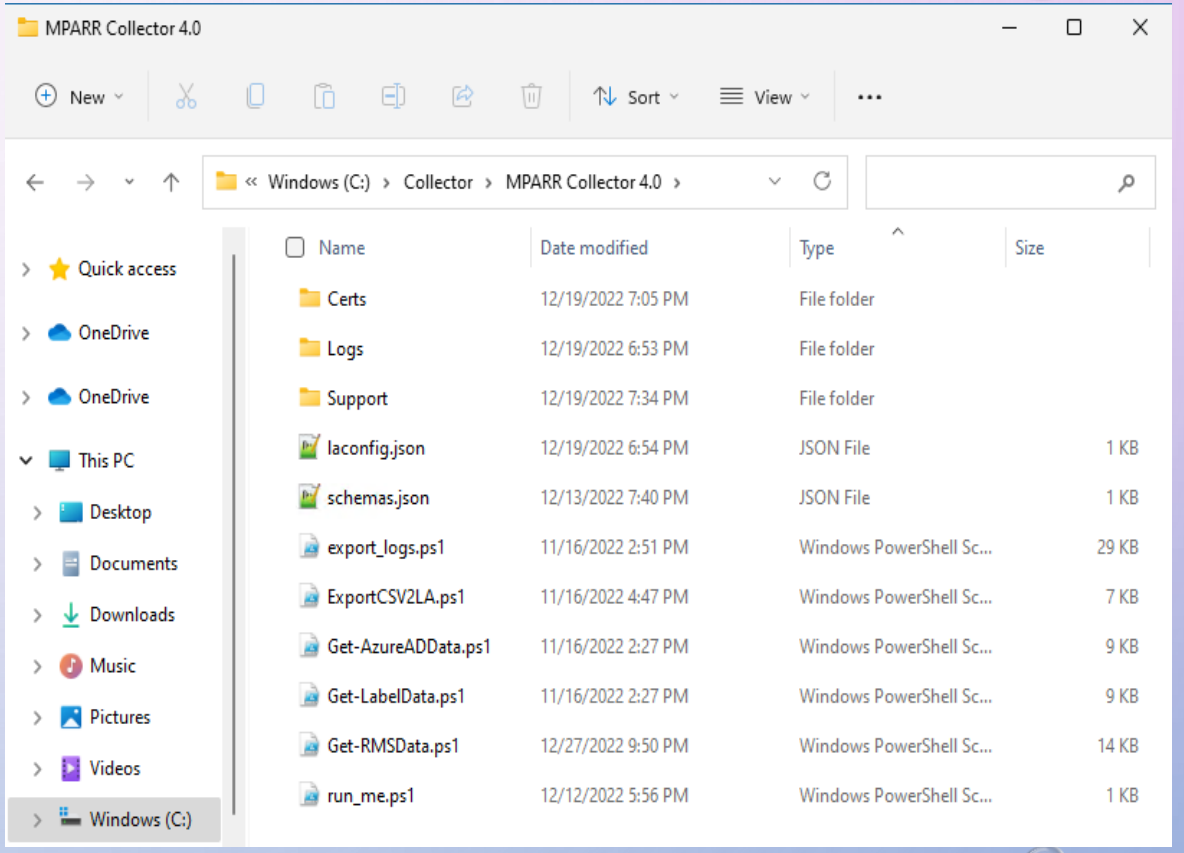
EXPORTCSV2LA.PS1: SCRIPT USED TO EXPORT THE CSV FILE (LOCATED ON SUPPORT FOLDER) WITH SERVICE PLAN TO LOGS ANALYTICS (REQUIRED TO EXECUTE ON-DEMAND)

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)

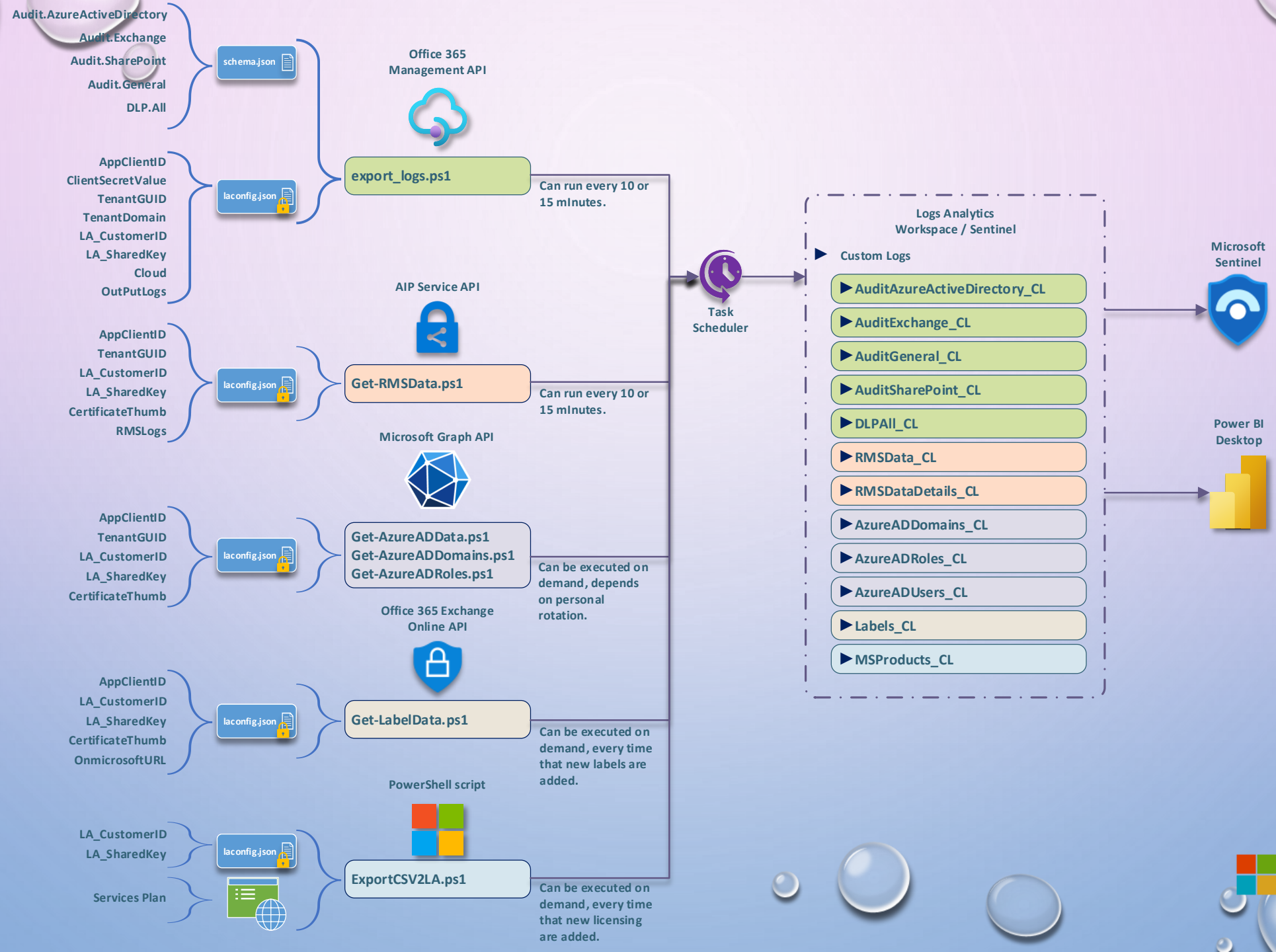
GET-RMSDATA.PS1: SCRIPT USED TO OBTAIN INFORMATION ABOUT EXTERNAL ACCESS TO PROTECTED FILES, REQUIRE AIPSERVICE POWERSHELL MODULE, PERMISSIONS ARE ADDED TO AZURE AD APP FOR UNATTENDED EXECUTION (RECOMMEND TO EXECUTE AT LEAST DAILY) – **UNDER CONSTRUCTION**

RUN_ME.PS1: SCRIPT USED TO CALL EXPORT_LOGS.PS1 WITH PARAMETERS TO USE WITH TASK SCHEDULER

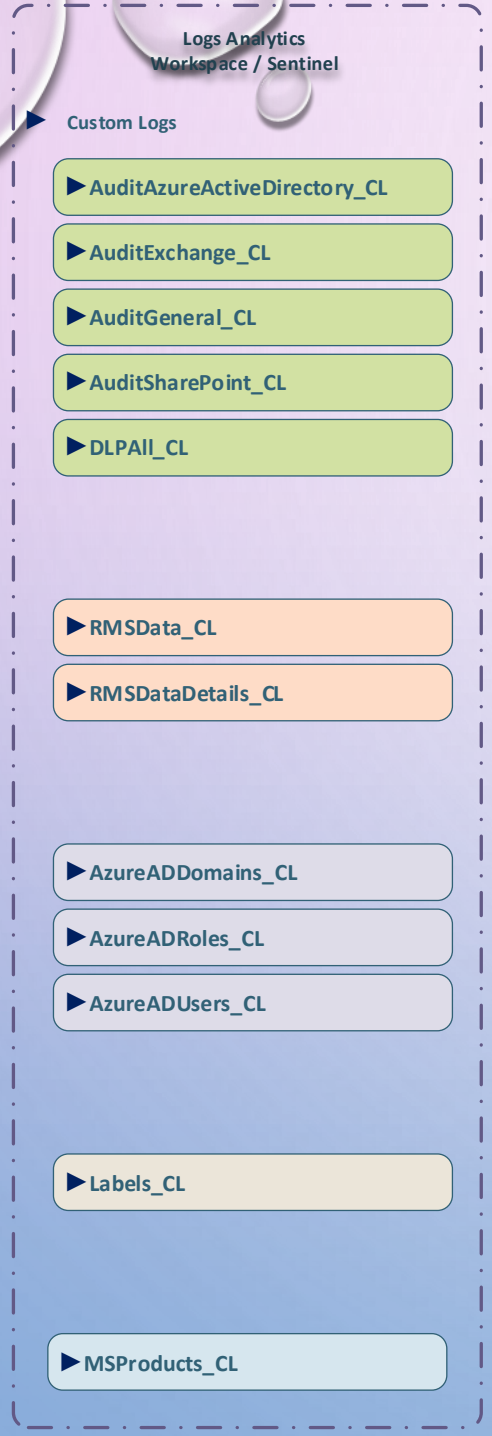


Microsoft

DETAILED ARCHITECTURE



DETAILED ARCHITECTURE



Used to collect all the data from Office 365 Management API, according to this documentation.

The principal information collected permit to create all the dashboards based on the Operation field. The information collected permit to identify activities from end-users, admin users, and services accounts

Used to collect data from AIP Service API, this permit to collect information related to external access to protected documents, and information related to denied access to protected documents from internal or external access.

This information permit create dashboards for Unified Labeling to identify access denied over protected documents for internal or external users, and detailed information for access to protected documents from external users.

Used to collect data from Microsoft Graph API, this information permit to identify Users, Admin roles, Domains registered on the Tenant, and Azure AD attributes.

This information permit to identify activities from specific roles, identify the domains registered on the Tenant, this permit to identify external access, and add filters based on Azure AD Attributes, like as, Department, Location, Countries, and all the attributes available and populated.

Used to collect data from Office 365 Exchange Online API, this information permit identify Labels Names and Priority for these labels.

Used to create reports for Unified Labeling, collecting Display Name of the labels and Parent Display Name, this last is for Sub-Labels, this permit to show the names of the Labels on Unified Labeling reports, the display name is not available under Office 365 Management API.

This table collect the information related to friendly names for licensing.

Under Azure AD the licensing is showing with an ID or a short name that is not friendly to identify the right one, for that reason this data permit to see the friendly names on reports.

PREREQUISITES

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

Microsoft

INDEX

GO DIRECTLY FROM HERE TO THE SPECIFIC TOPICS

Microsoft

AZURE AD

CREATE APP TO RECOLLECT DATA (1/2)

- OPEN 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
  - 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.

Microsoft

AZURE AD

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”

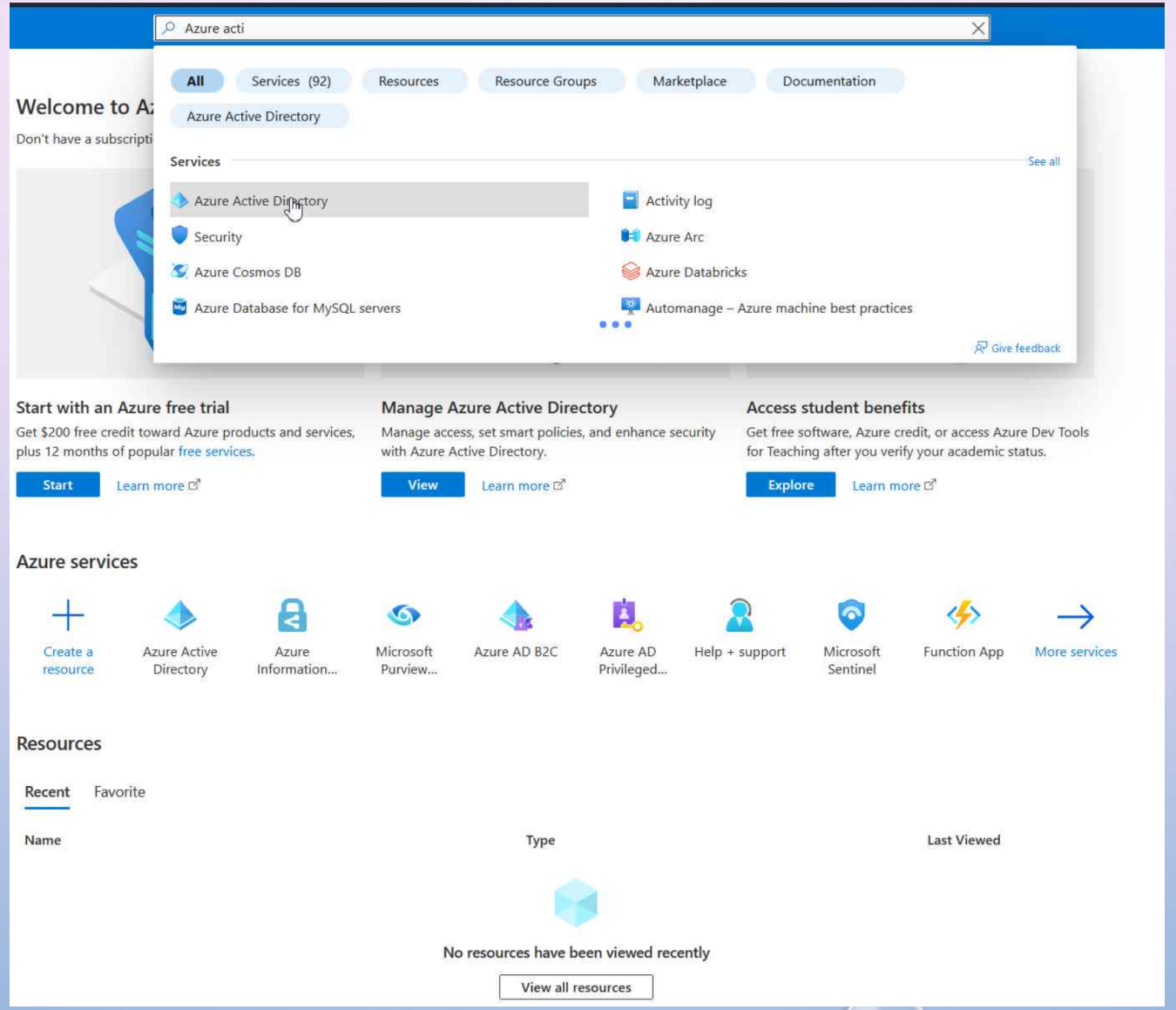
    TO GIVE ACCESS TO AIP SERVICE API (AZURE RIGHTS MANAGEMENT SERVICES)

    - 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

Microsoft

AZURE AD

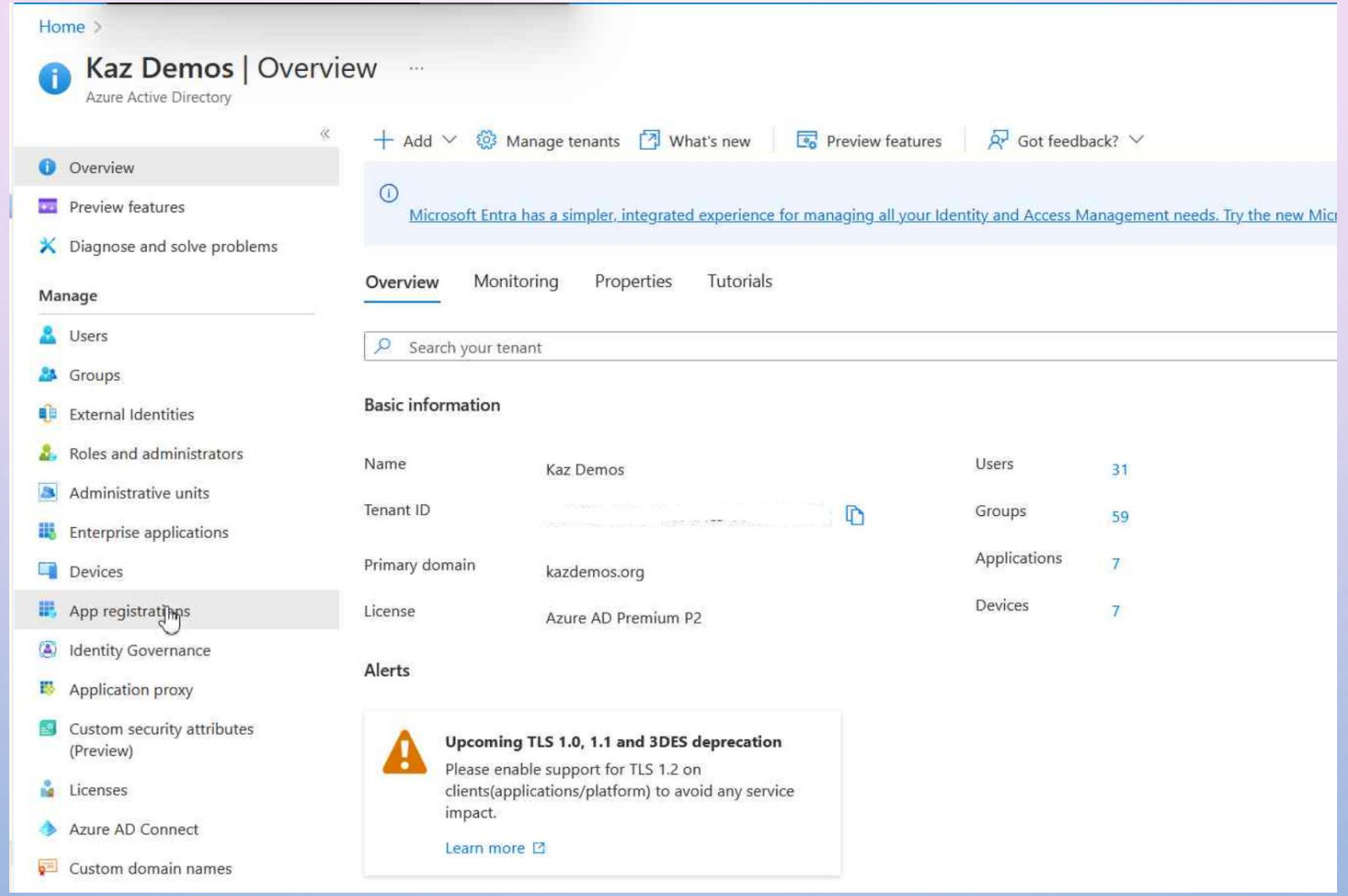
STEPS



Microsoft

AZURE AD

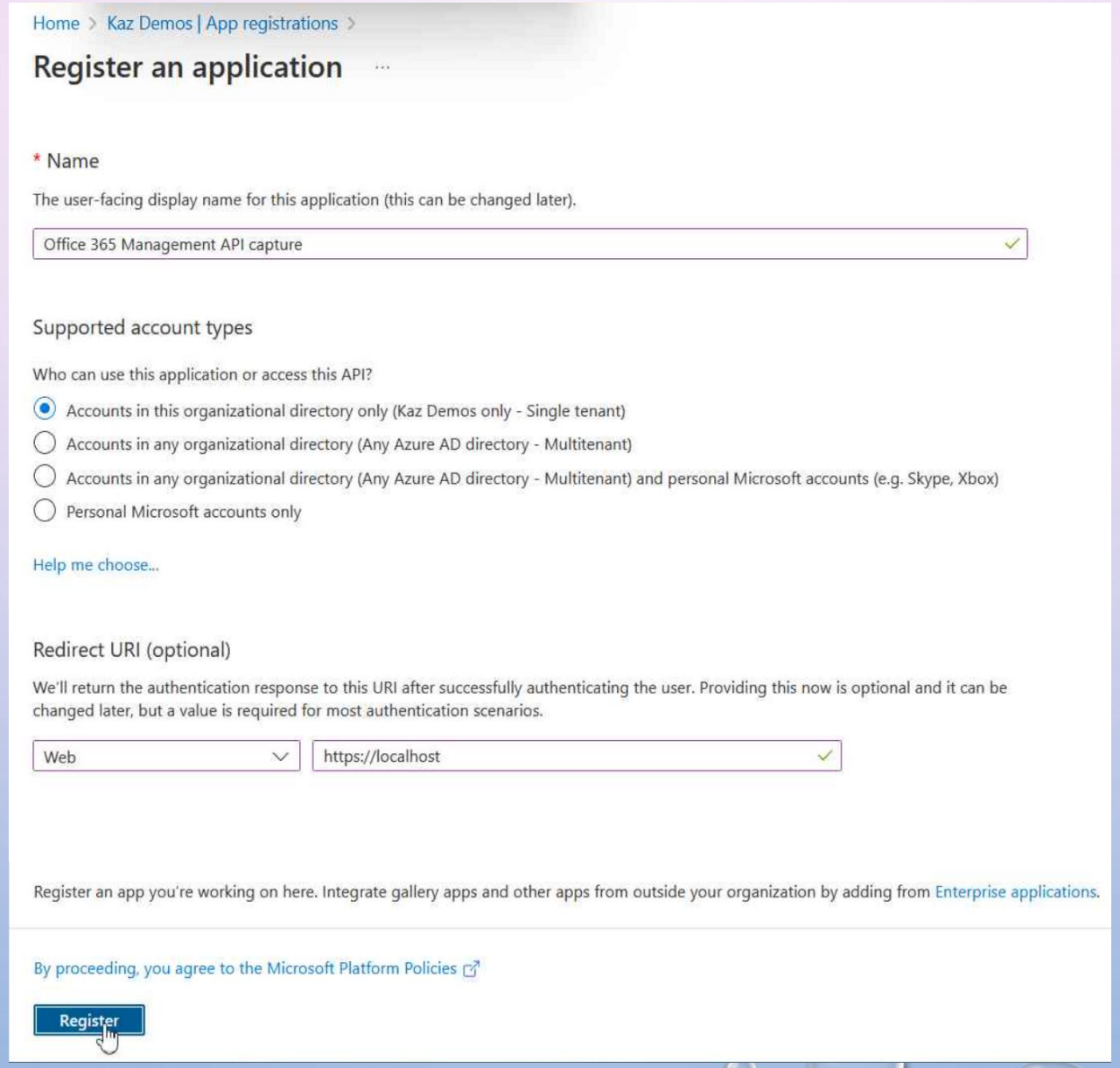
STEPS



Microsoft

AZURE AD

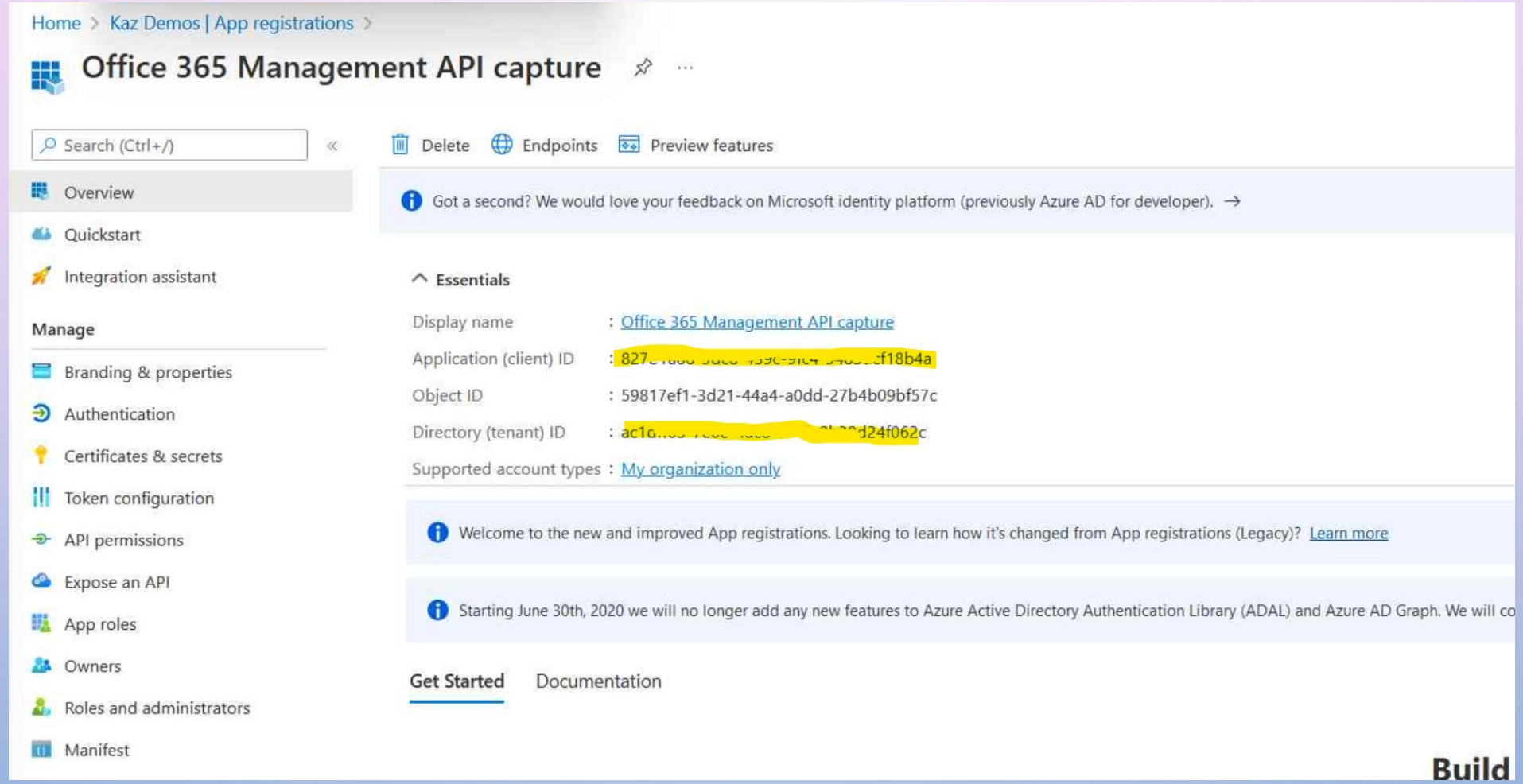
STEPS



Microsoft

AZURE AD

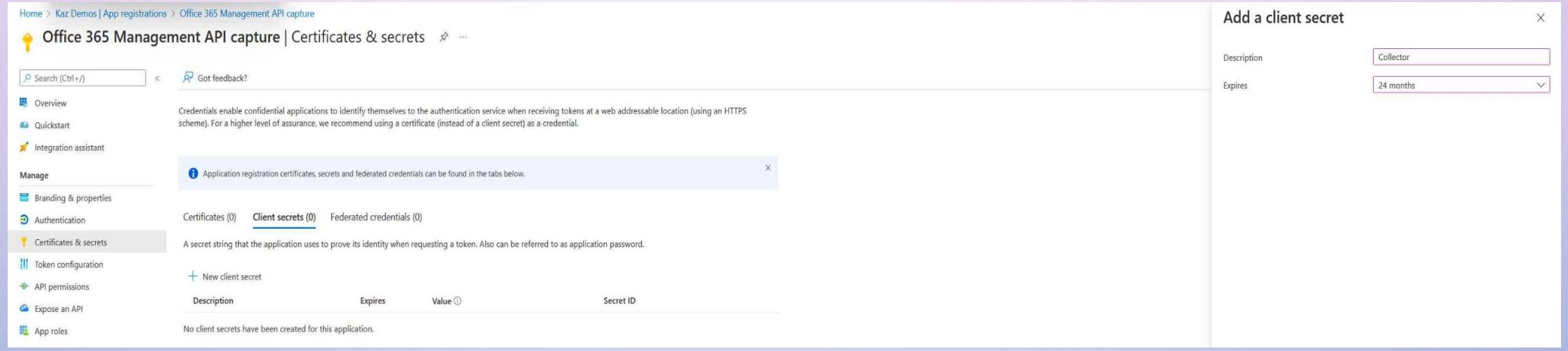
STEPS



Microsoft

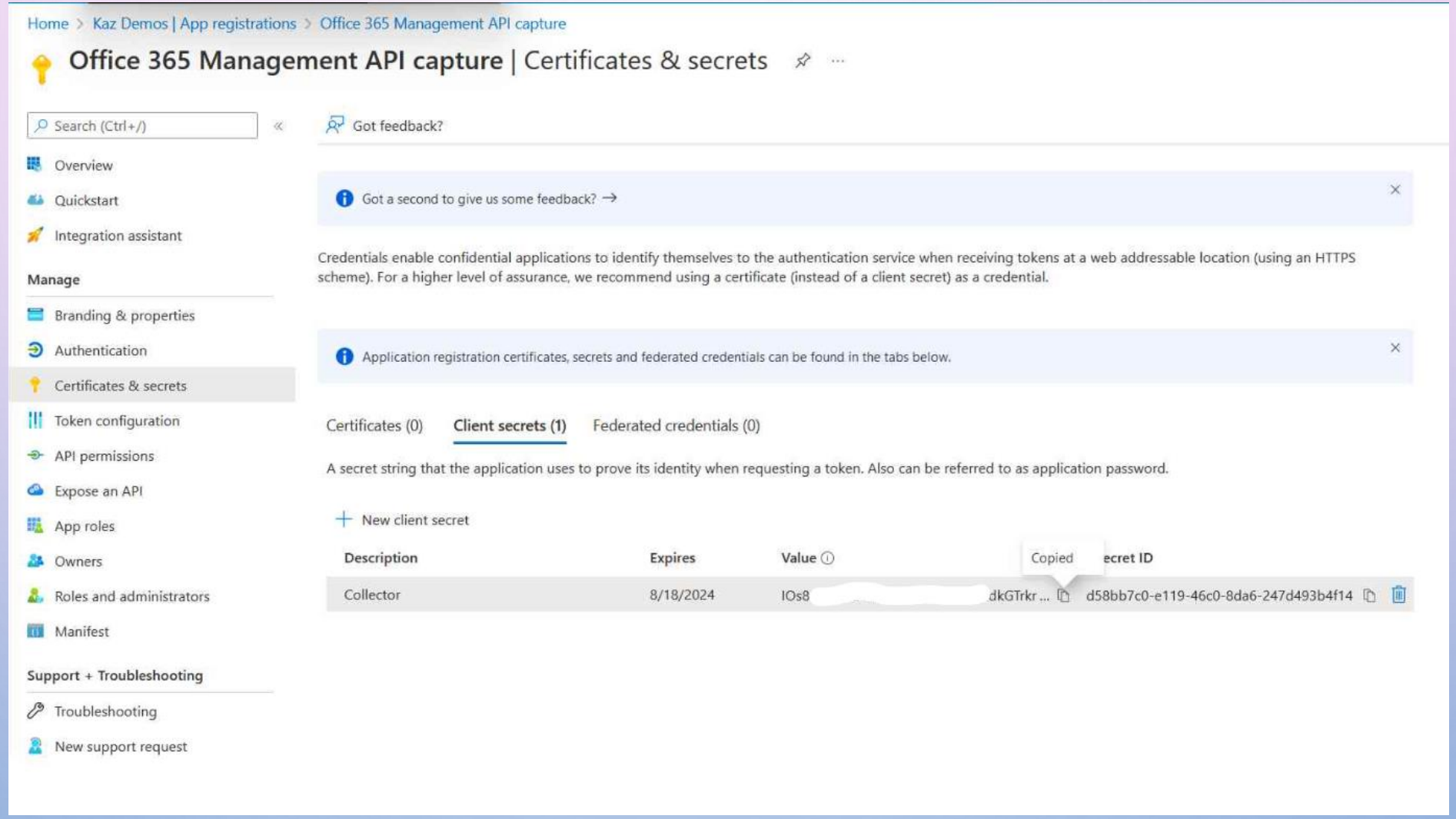
AZURE AD

STEPS



AZURE AD

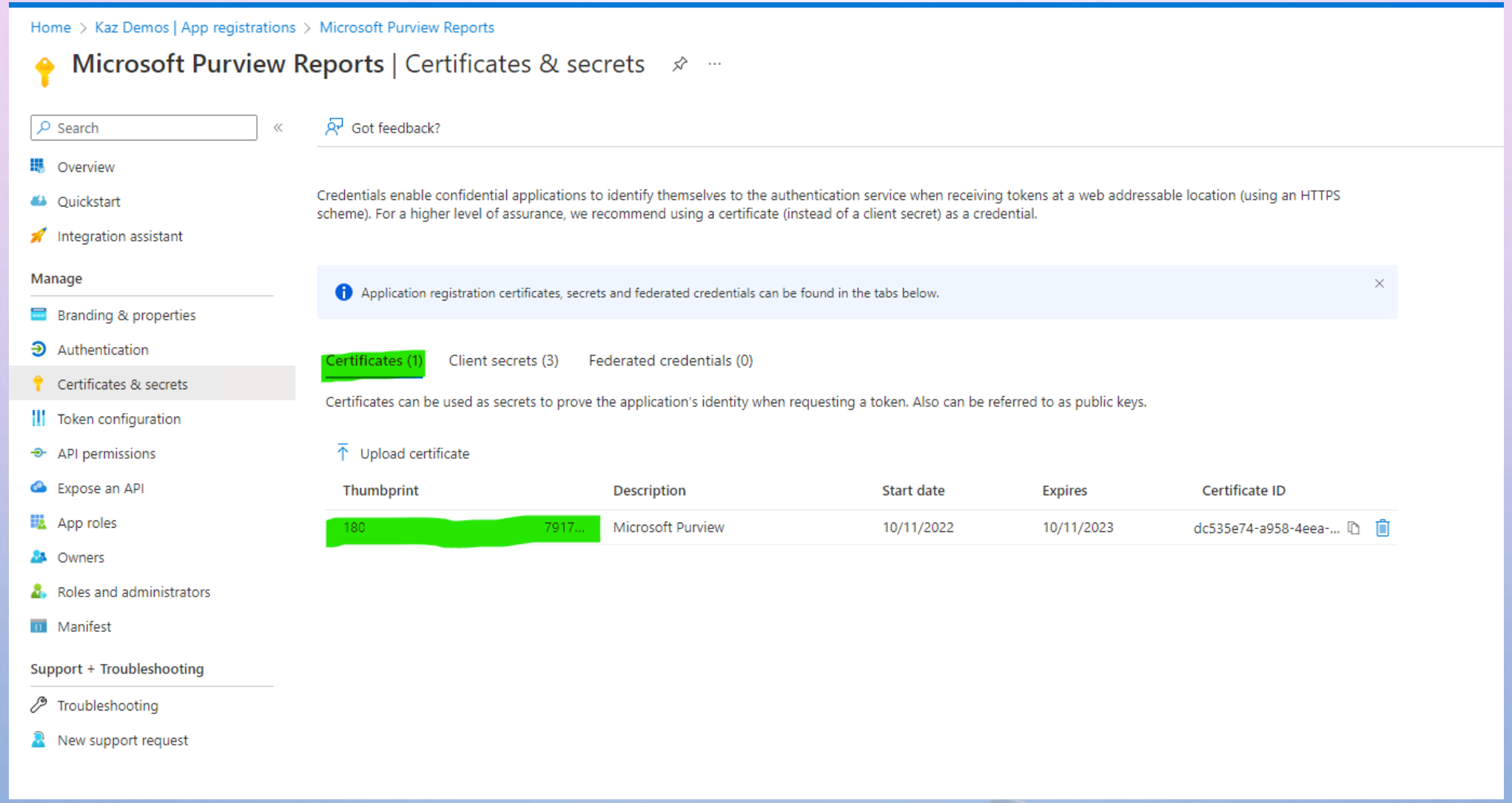
STEPS



Microsoft

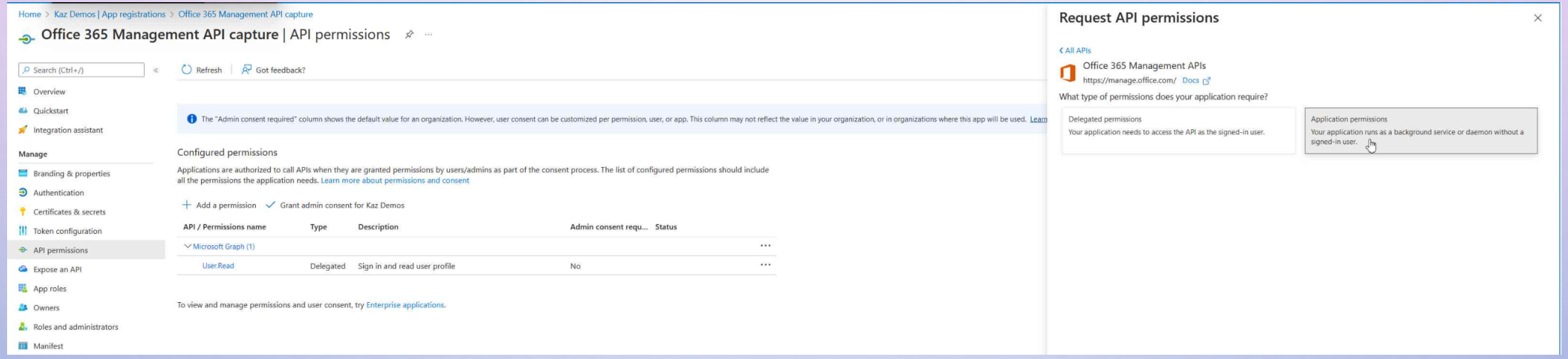
AZURE AD

STEPS



AZURE AD

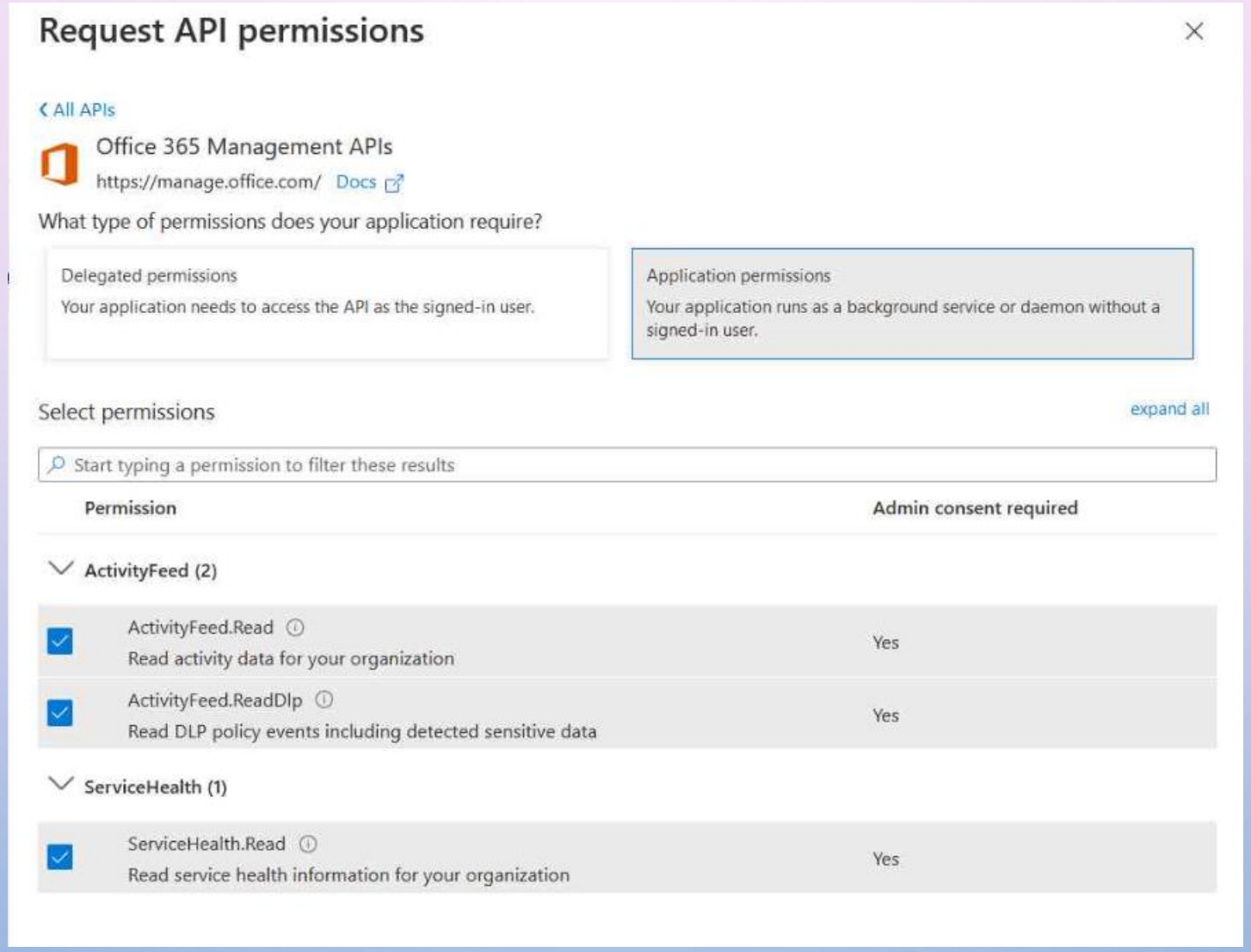
STEPS



Microsoft

AZURE AD

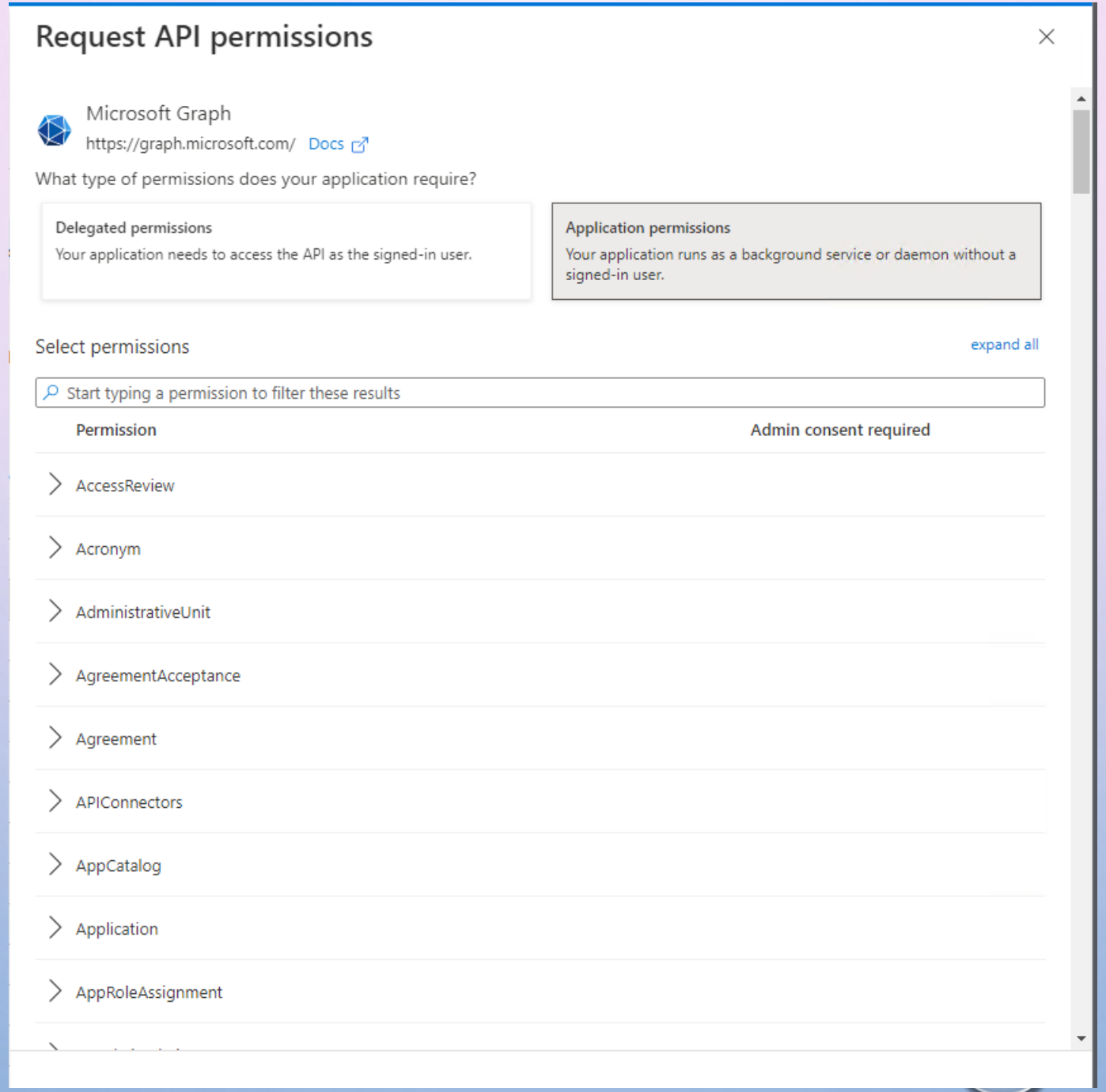
STEPS



Microsoft

AZURE AD

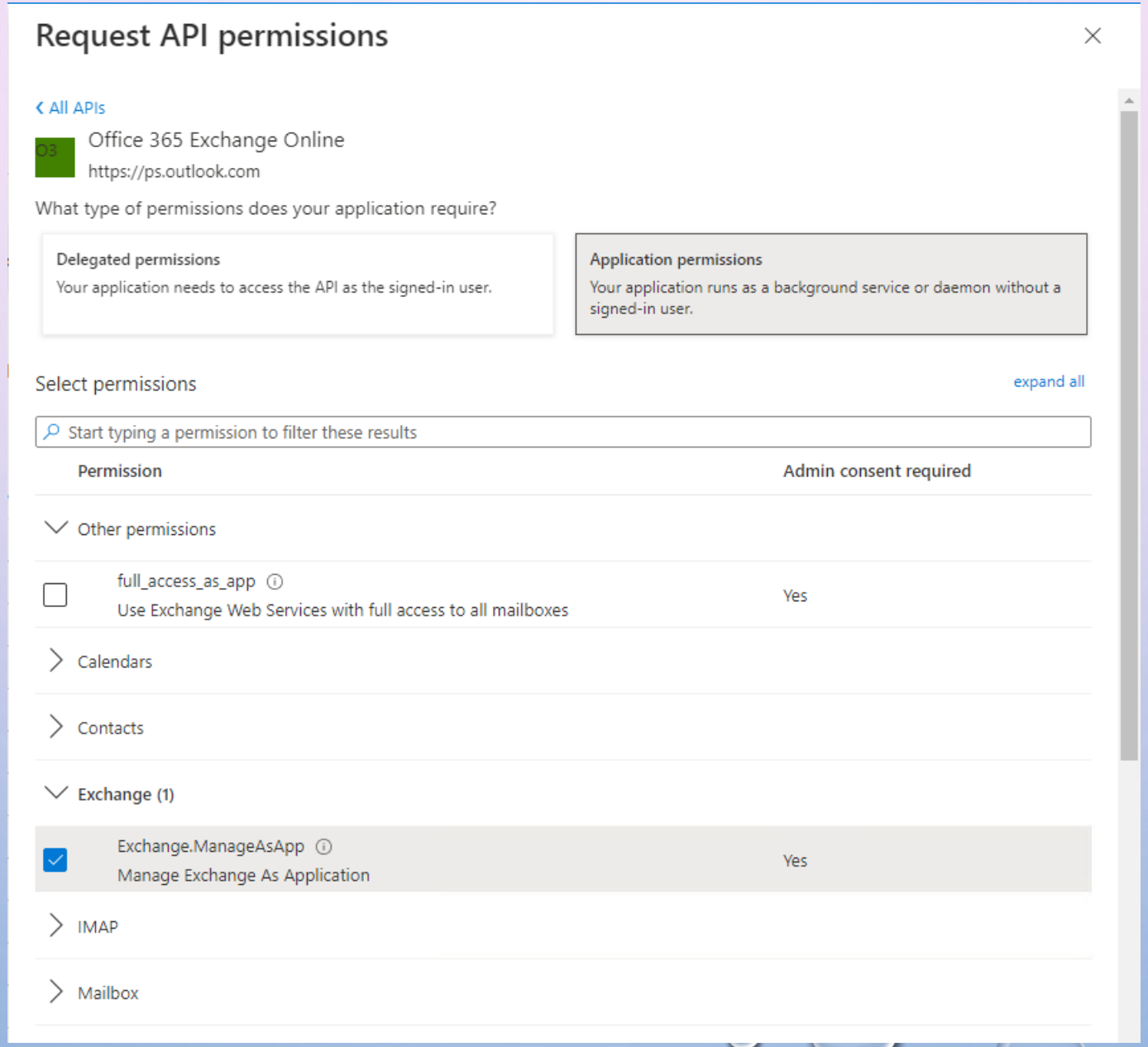
STEPS



Microsoft

AZURE AD

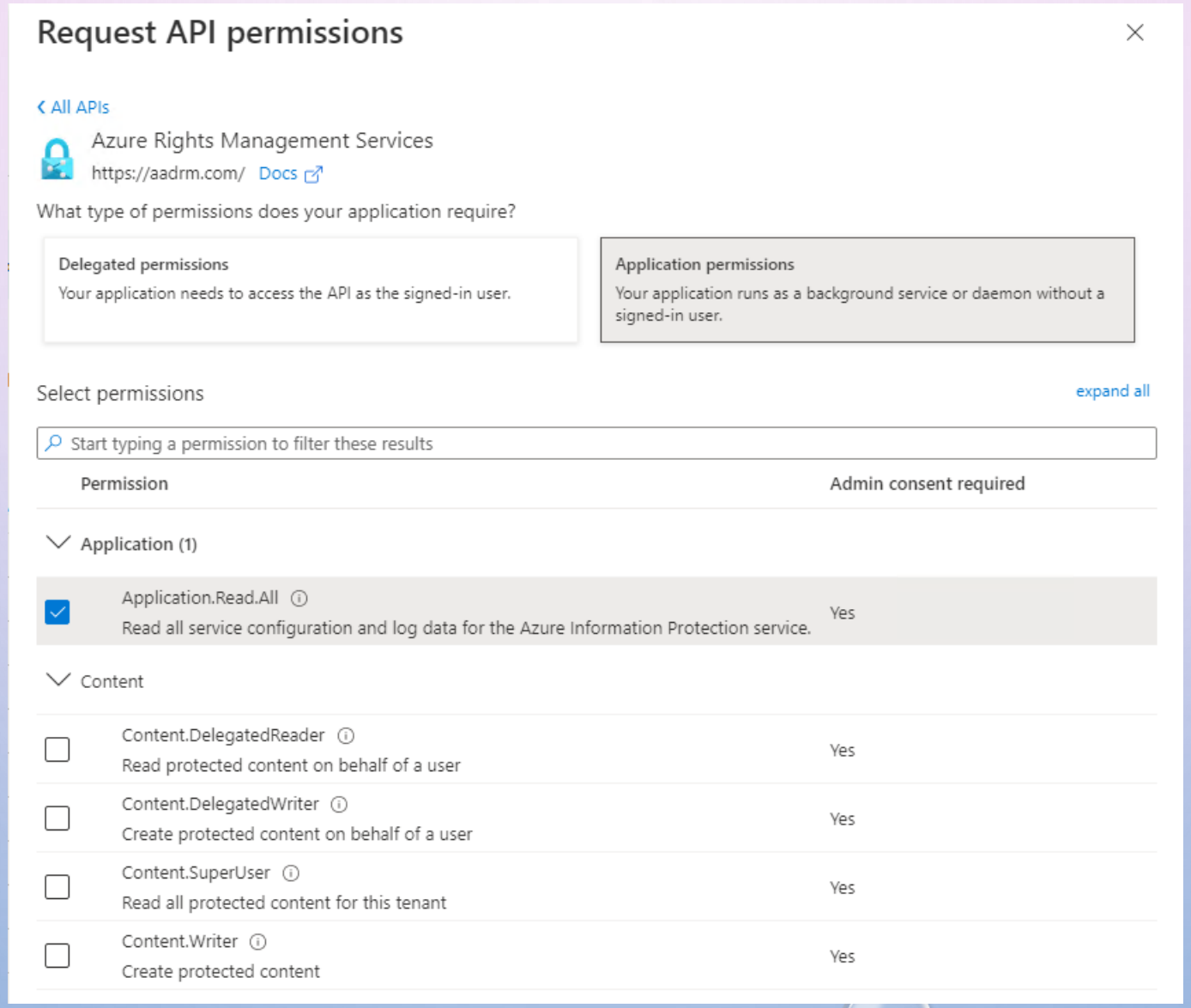
STEPS



Microsoft

AZURE AD

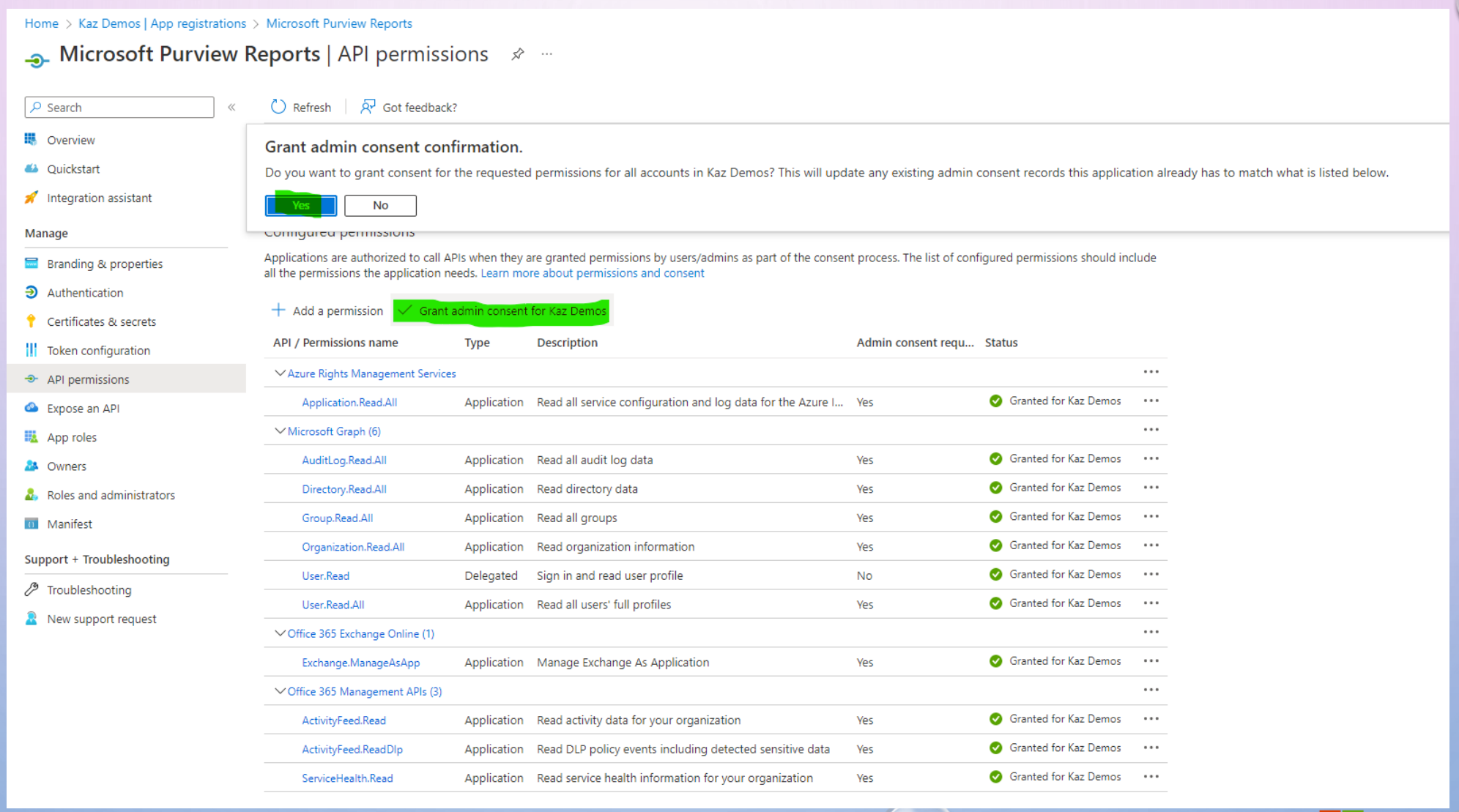
STEPS



Microsoft

AZURE AD

STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

CREATE A WORKSPACE IN LOGS ANALYTICS

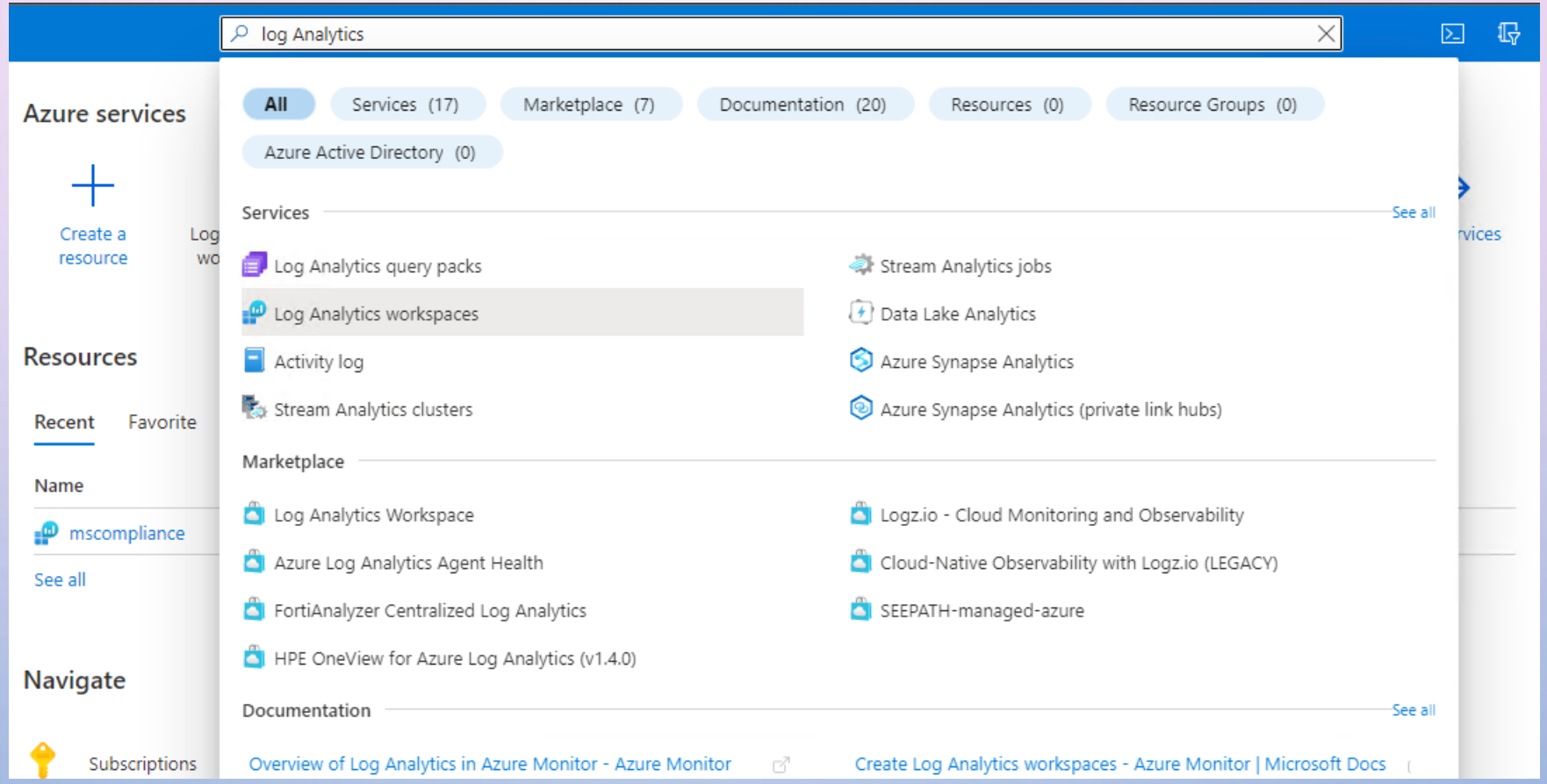
- OPEN HTTPS://PORTAL.AZURE.COM
- LOOK FOR LOG ANALYTICS WORKSPACES
- PRESS +CREATE
  - SELECT YOUR AZURE SUBSCRIPTION
  - SELECT OR CREATE A RESOURCE GROUP
  - SET A NAME RELATED TO THIS WORKSPACE
  - SELECT THE REGION THAT BEST MATCH
  - PRESS REVIEW + CREATE, WAIT UNTIL A RESUME IS SHOW
  - PRESS 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.

Microsoft

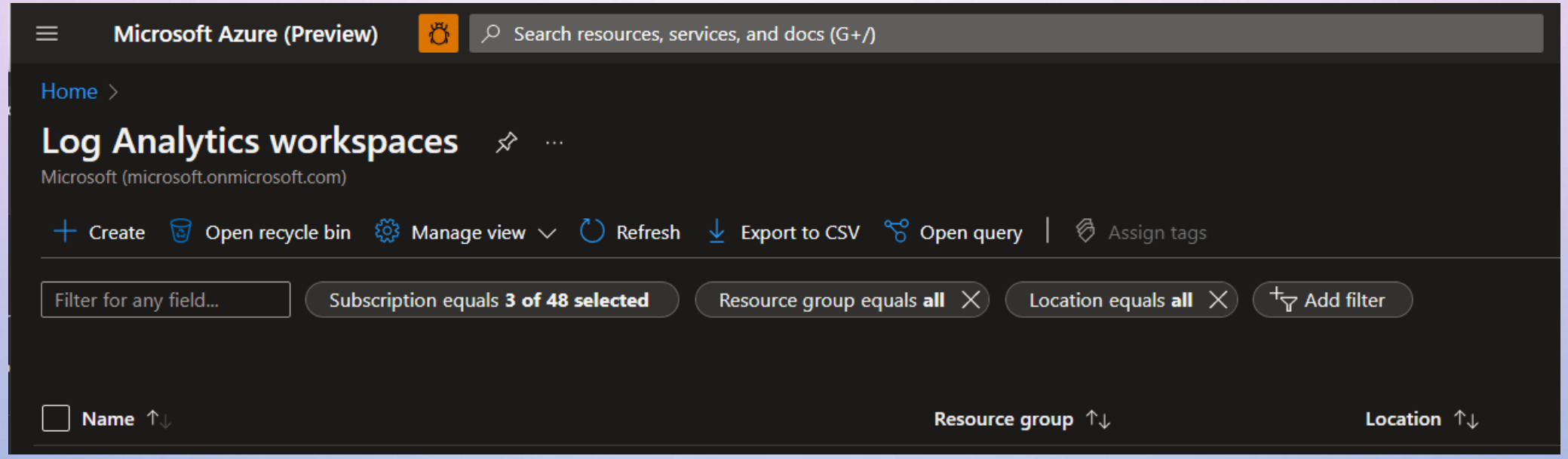
LOGS ANALYTICS WORKSPACE

STEPS



LOGS ANALYTICS WORKSPACE

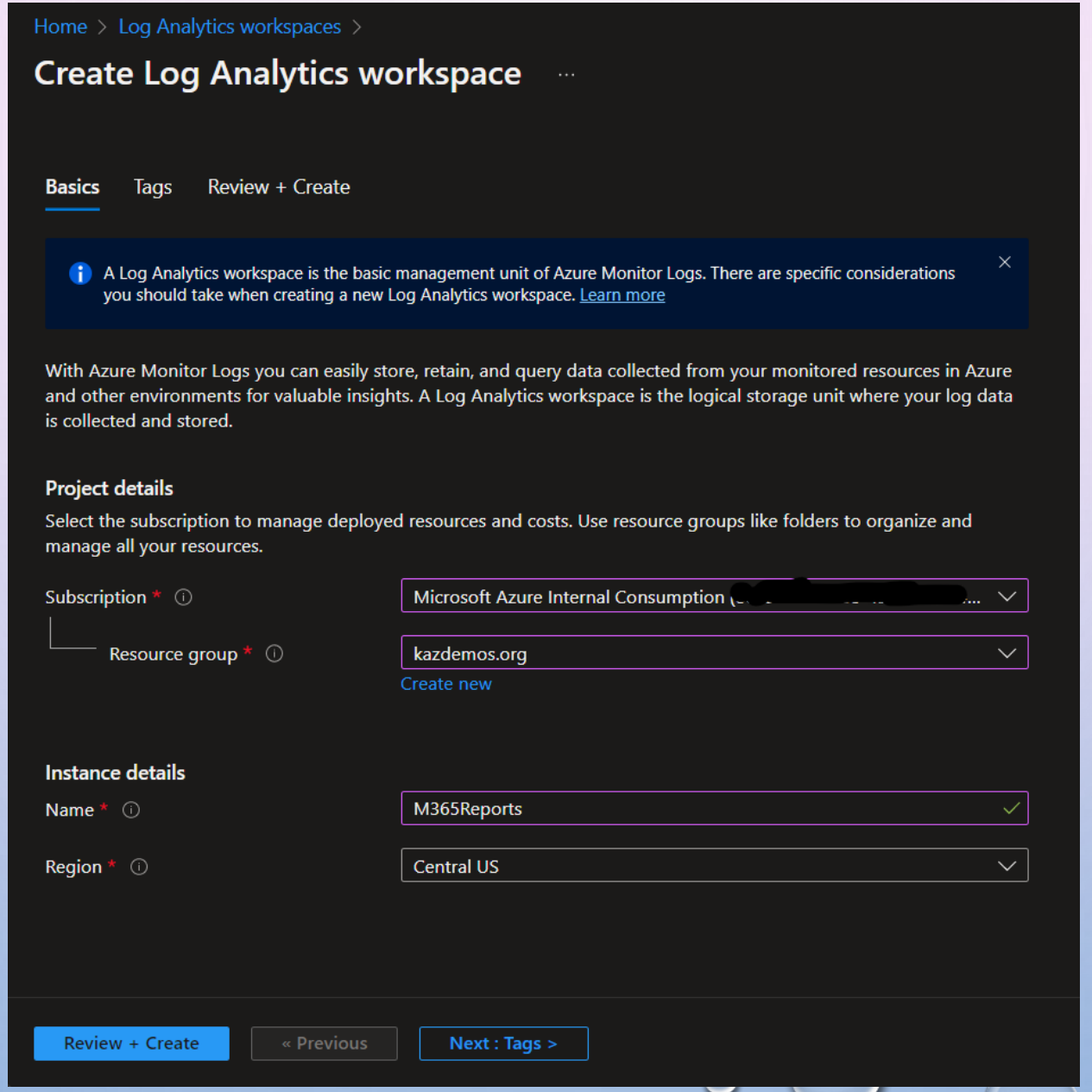
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

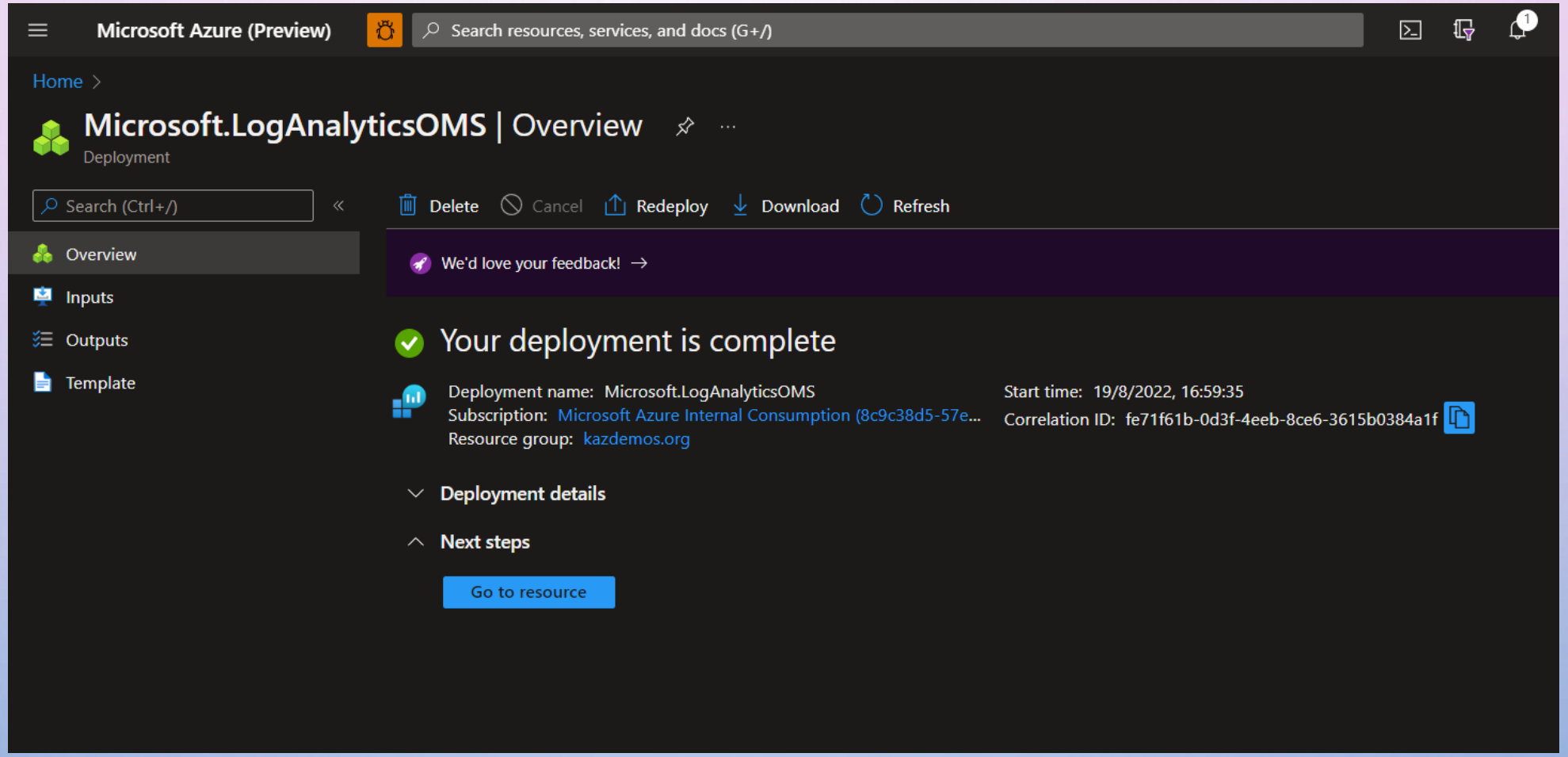
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

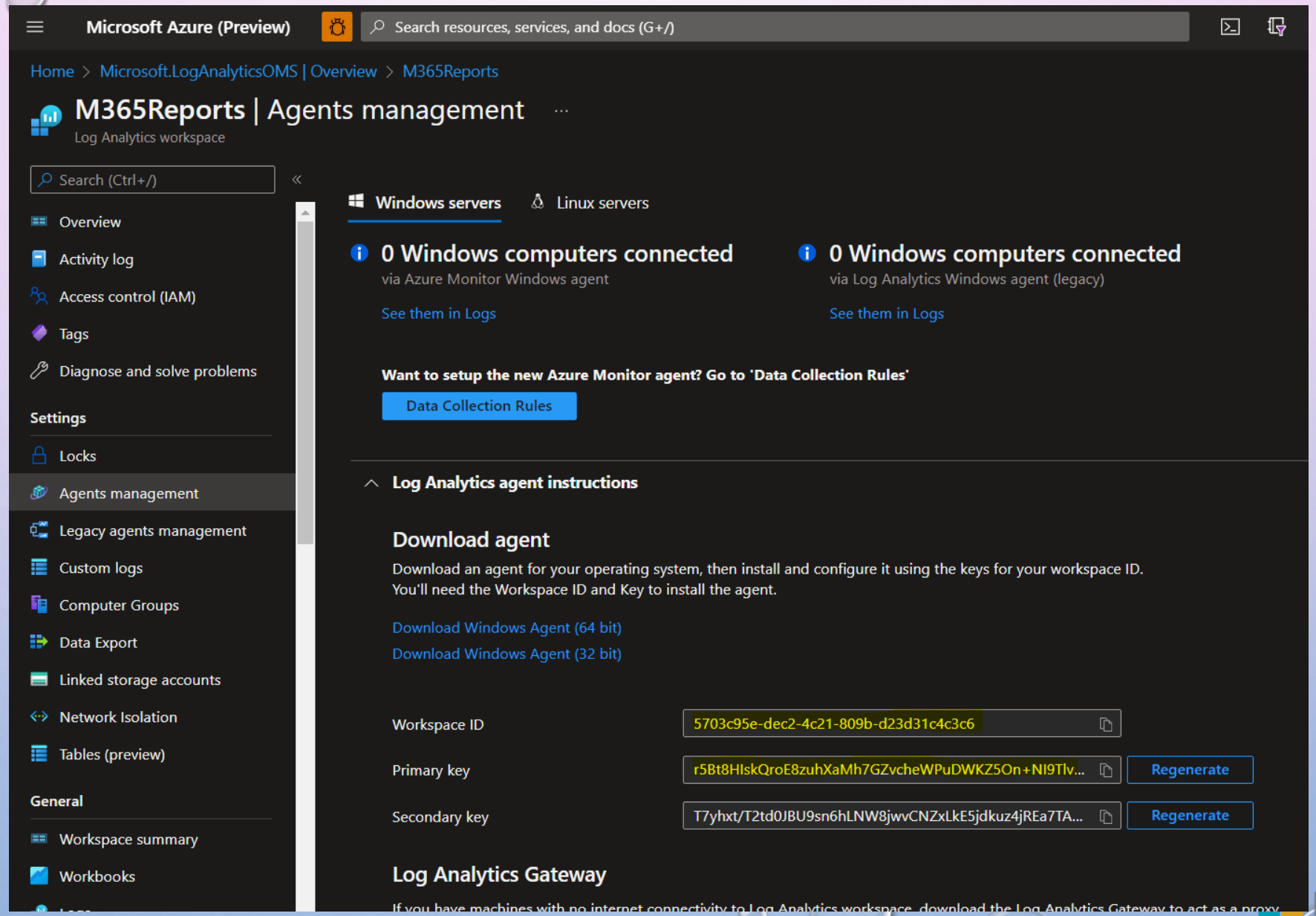
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

STEPS

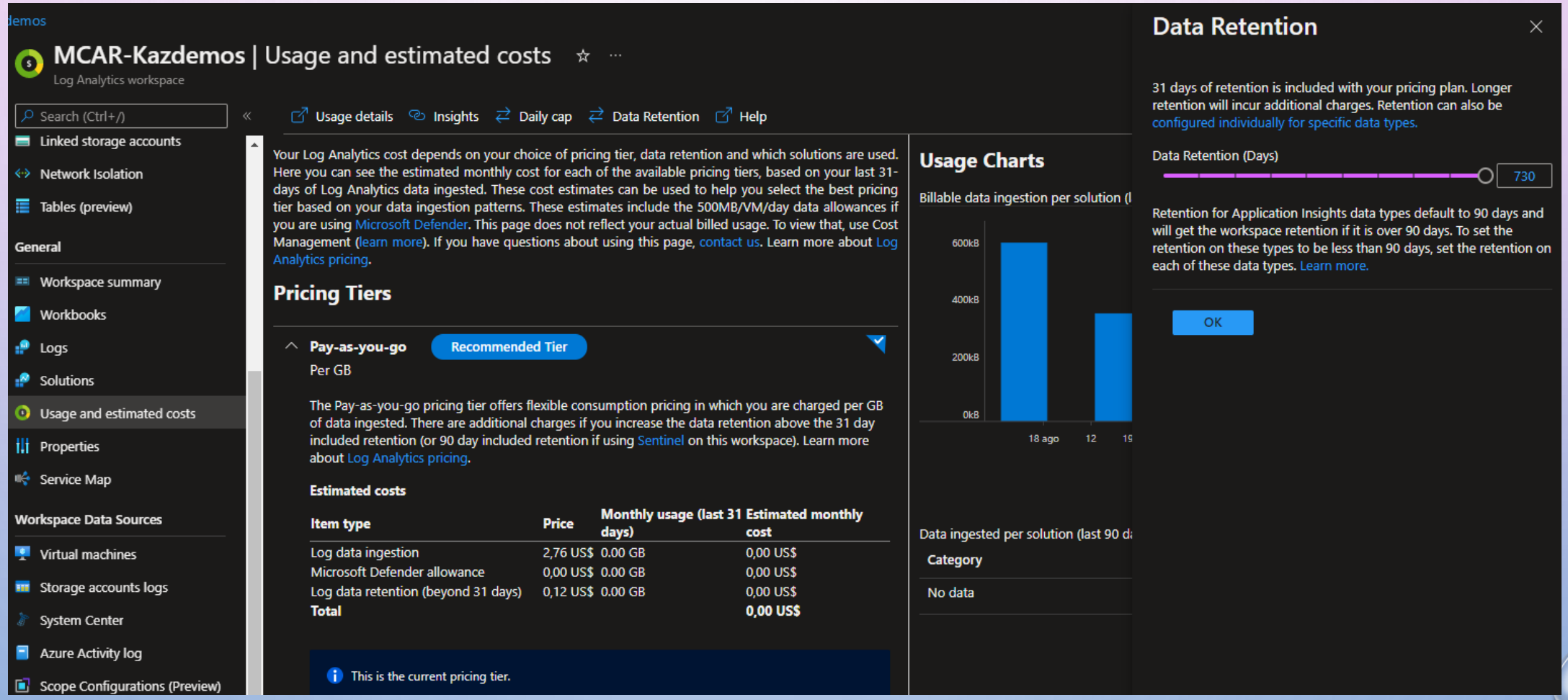


Microsoft

LOGS ANALYTICS WORKSPACE

EXTEND YOUR DATA RETENTION UNTIL 2 YEARS

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



GENERATE A CERTIFICATE TO EXECUTE SOME POWERSHELL CMDLETS UNATTENDED

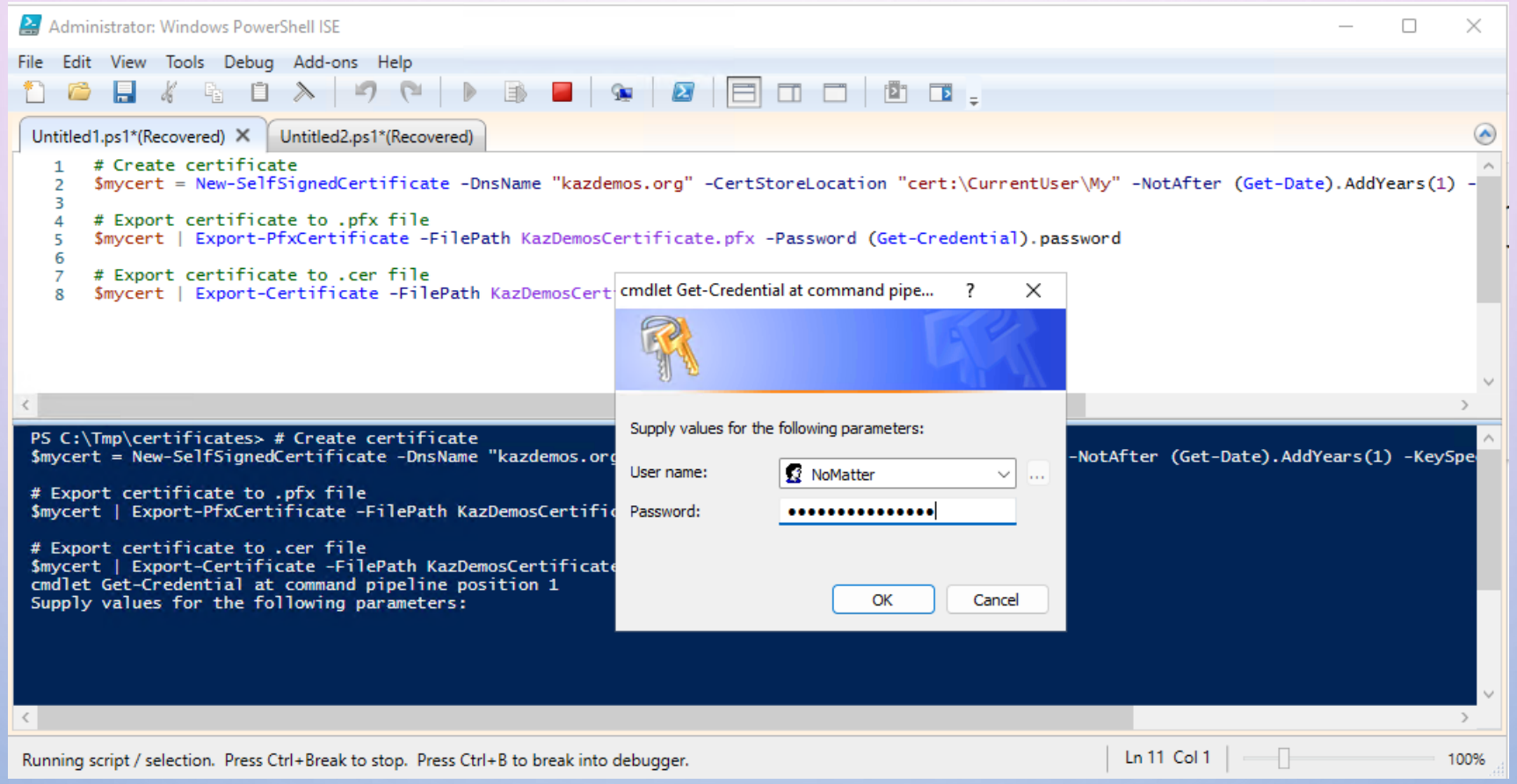
- WE WILL NEED TO **CREATE A CERTIFICATE** TO CONNECT TO INFORMATION PROTECTION SERVICES THROUGH AZURE AD APPLICATION, TO DO THAT THE 1ST STEP IS CREATE THAT CERTIFICATE:
  - OPEN AN ISE POWERSHELL CONSOLE AND EXECUTE (SELECT A FOLDER 1ST TO SAVE THE 2 FILES CREATED, EXAMPLE C:\TMP):

```
# CREATE CERTIFICATE
$MYCERT = NEW-SELFSIGNEDCERTIFICATE -DNSNAME "KAZDEMOS.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

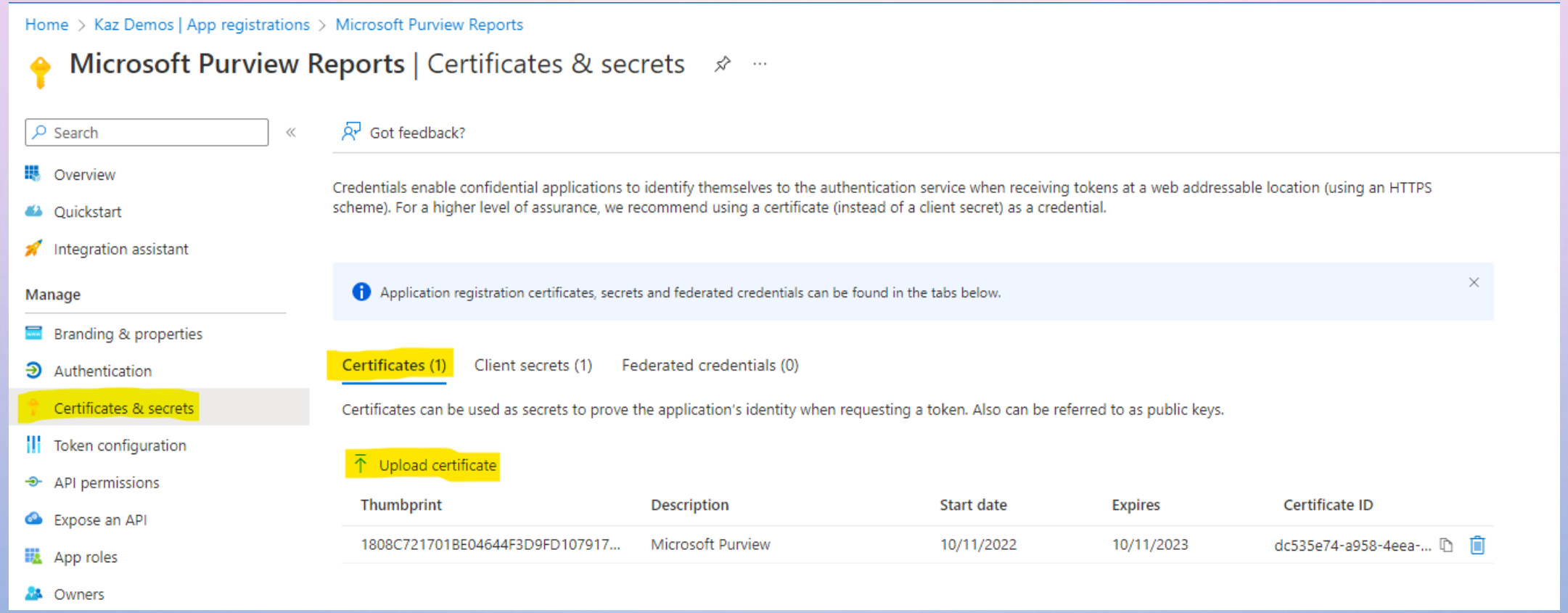
STEPS



Microsoft

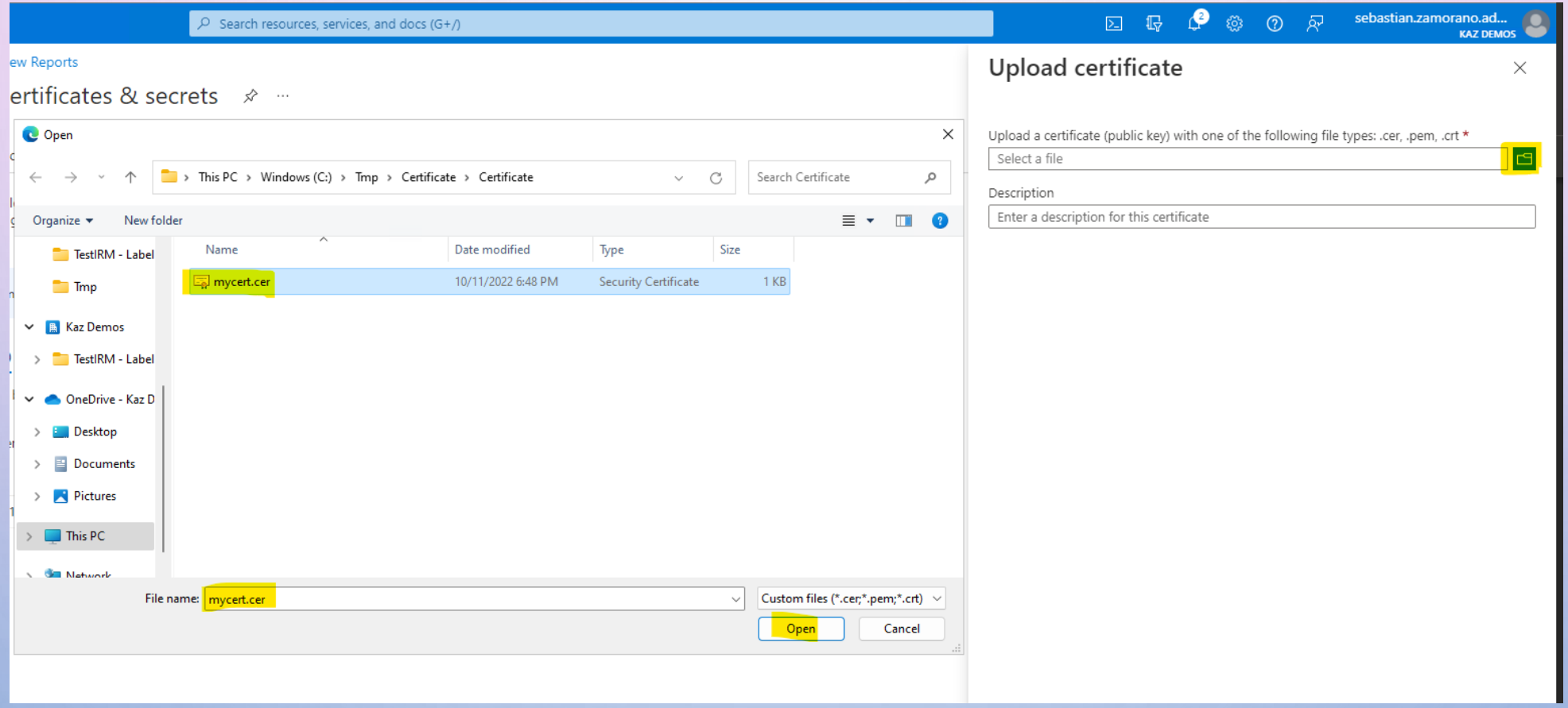
ADD CONFIGURATION TO AZURE AD APP

STEPS



ADD CONFIGURATION TO AZURE AD APP

STEPS



Microsoft

ADD CONFIGURATION TO AZURE AD APP

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 | new 2 | my_kazdemos_labels.csv | new 3 | new 4 | run_me.ps1 | new 5 | Get-auditLogs.ps1 | export_logs.ps1 | Get-LabelData.ps1 | laconfig.json | ExportCSV2LA.ps1

```
{
    "EncryptedKeys": "True",
    "AppClientID": "[illegible]-429f-8e13-[illegible]f20",
    "ClientSecretValue": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e3000000
    "TenantGUID": "[illegible]-4ac8-a4c9-[illegible]2c",
    "TenantDomain": "kazdemos.org",
    "LA_CustomerID": "[illegible]-1a38-[illegible]-adaf-[illegible]3",
    "LA_SharedKey": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e30000000002
    "CertificateThumb": "01000000d08c9ddf0115d1118c7a00c04fc297eb010000009be602676a73ec489a1075b1c814e1e30000000
    "OnmicrosoftURL": "M[illegible]36.onmicrosoft.com"
}
```

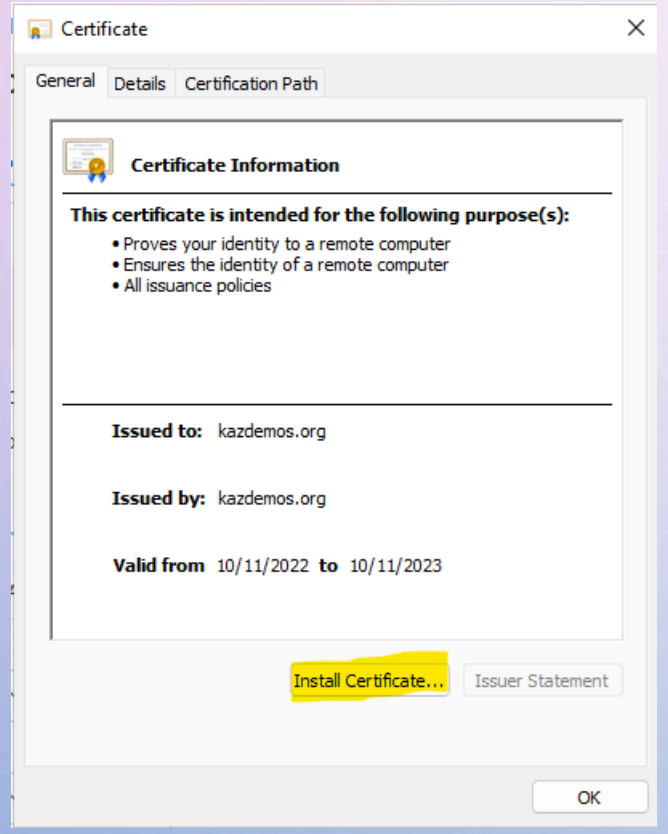
In this case the certificate thumbprint was encrypted using the steps explained in this slide

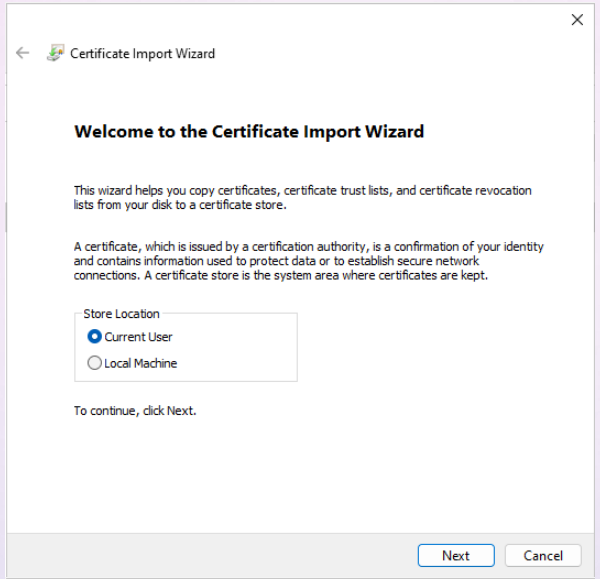
TO EXECUTE THE SCRIPT USING THE CERTIFICATE

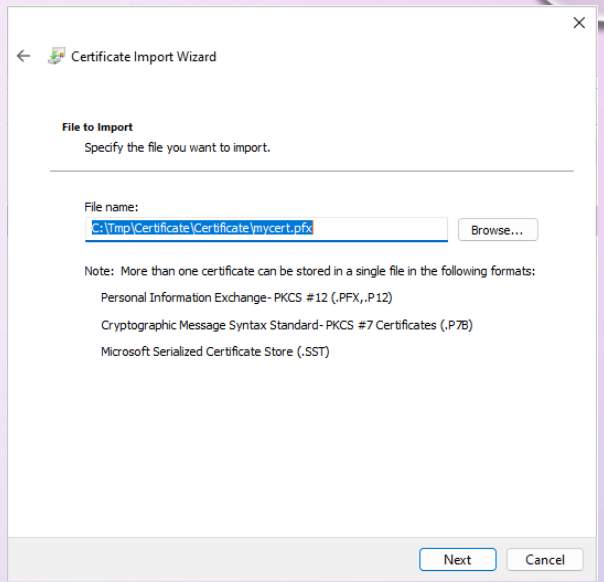
- ON THE SAME COMPUTER USED TO EXECUTE THE SCRIPTS IS NEEDED TO INSTALL BOTH CERTIFICATES PREVIOUSLY CREATED
- THE CERTIFICATES NEEDS TO BE INSTALLED ON THE SAME ACCOUNT USED TO EXECUTE THESE SCRIPTS:
  - GET-AZUREADDATA.PS1
  - GET-AZUREADDOMAINS.PS1
  - GET-AZUREADROLES.PS1
  - GET-LABELDATA.PS1
  - GET-RMSDATA.PS1
- 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.

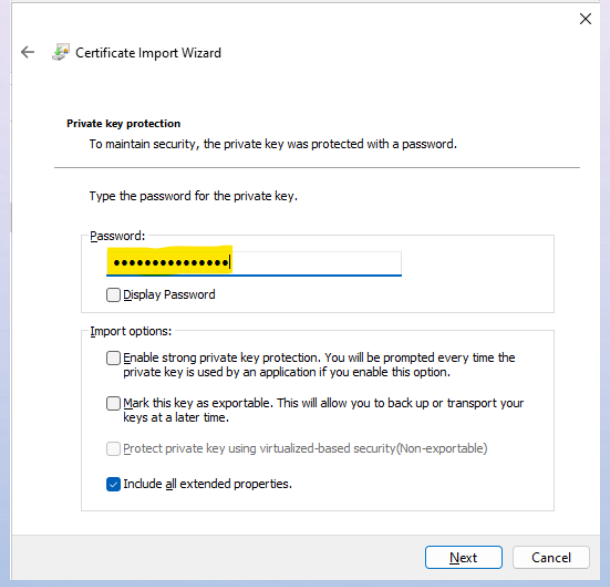
INSTALL CERTIFICATE LOCALLY

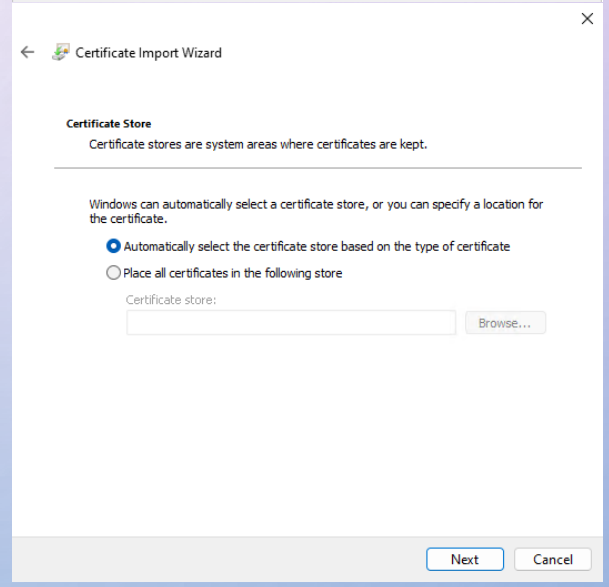
STEPS

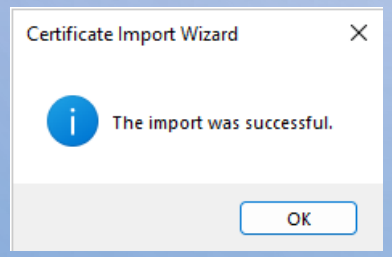












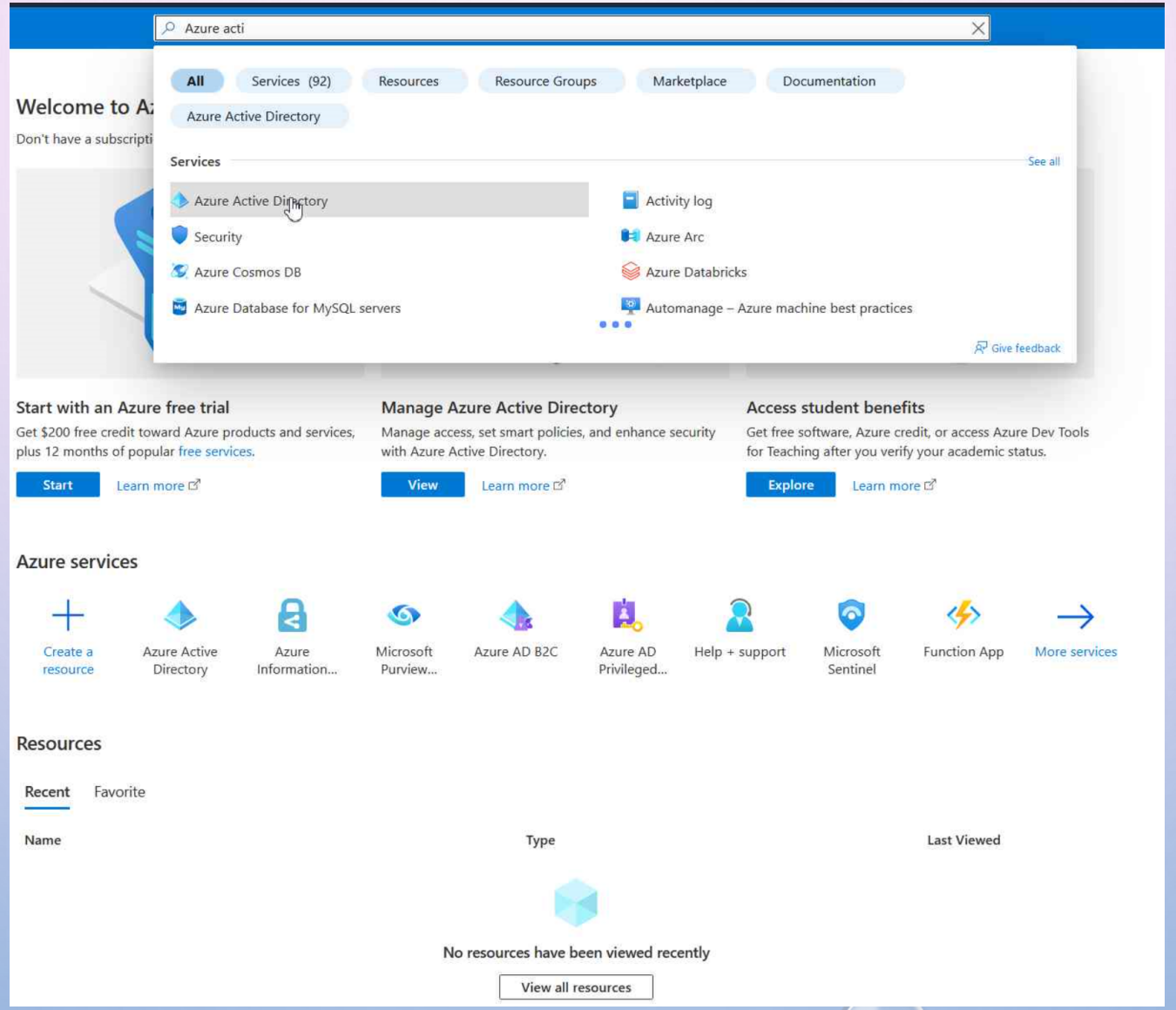
Microsoft

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

COMPLIANCE ADMIN ROLE FOR SCRIPT

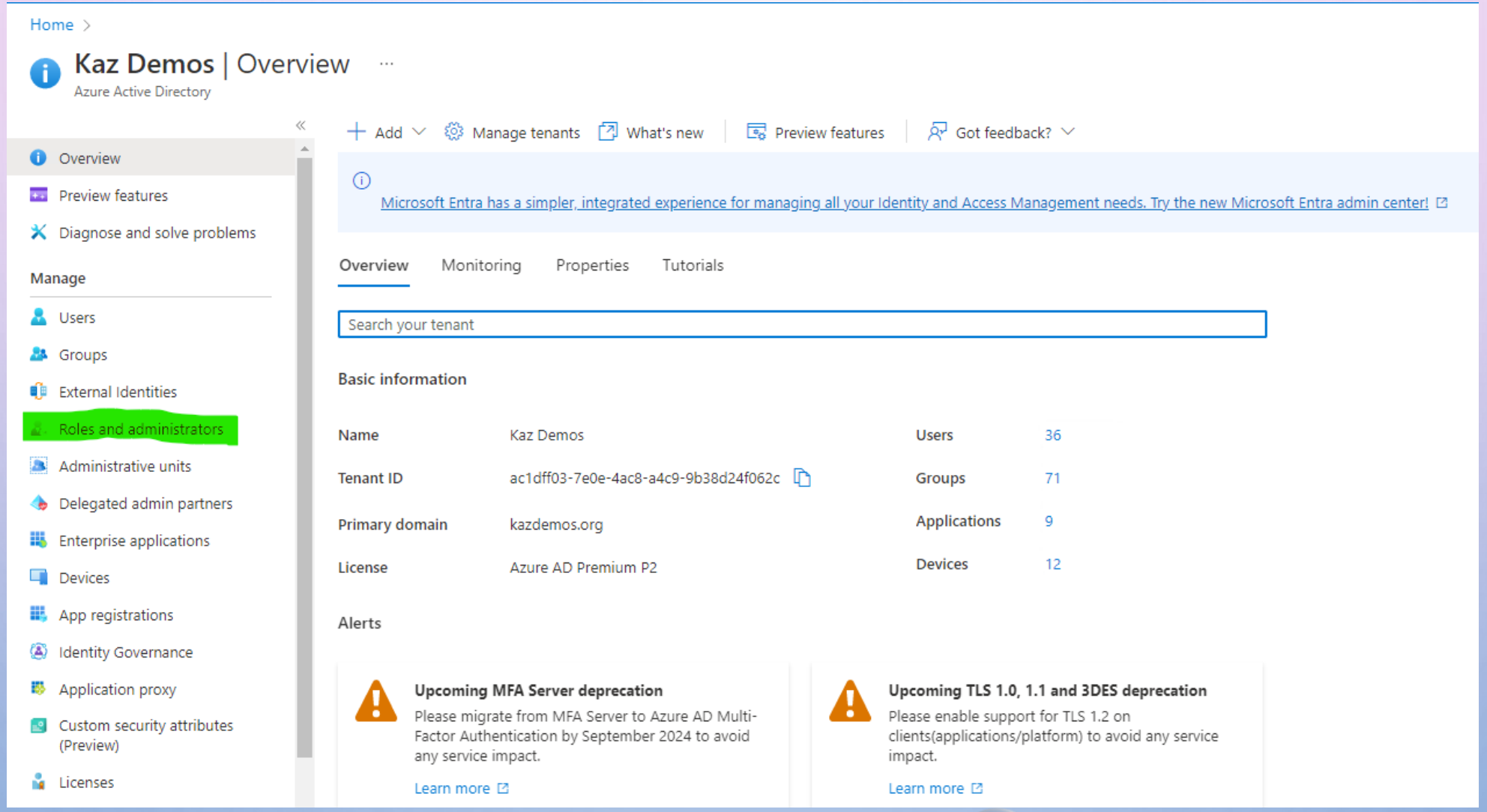
STEPS



Microsoft

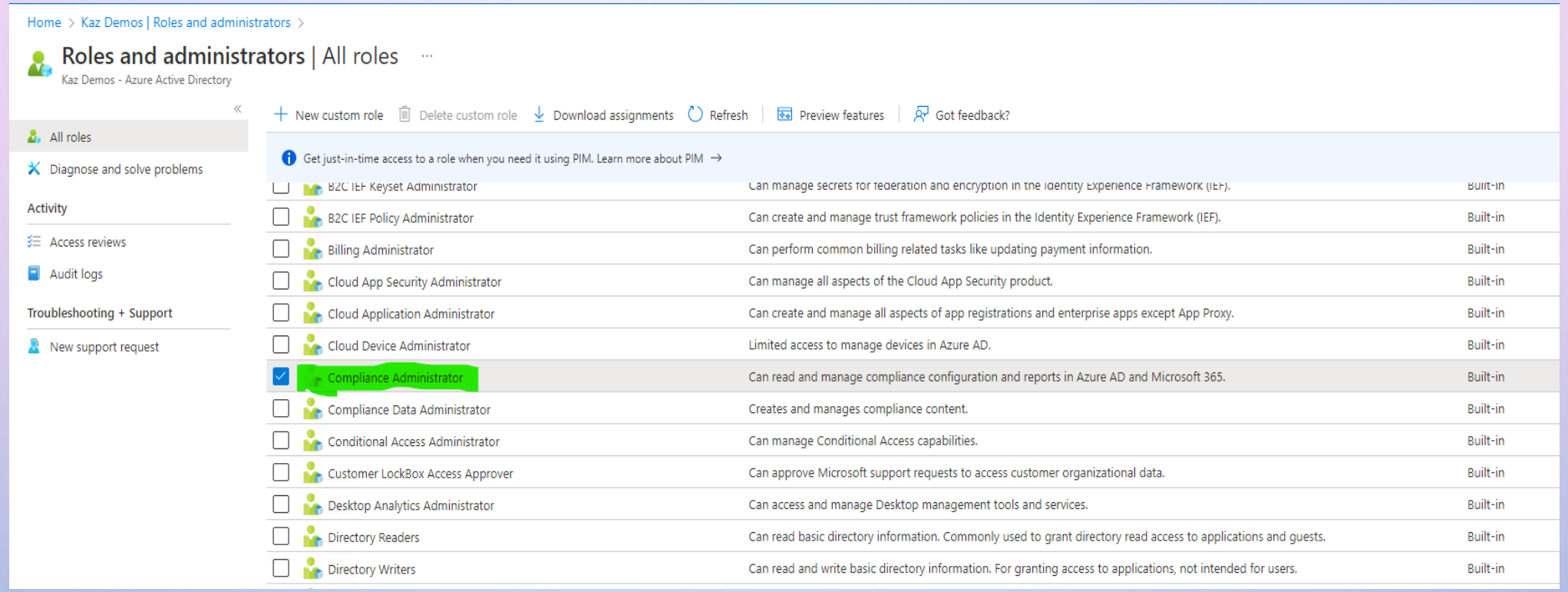
COMPLIANCE ADMIN ROLE FOR SCRIPT

STEPS



COMPLIANCE ADMIN ROLE FOR SCRIPT

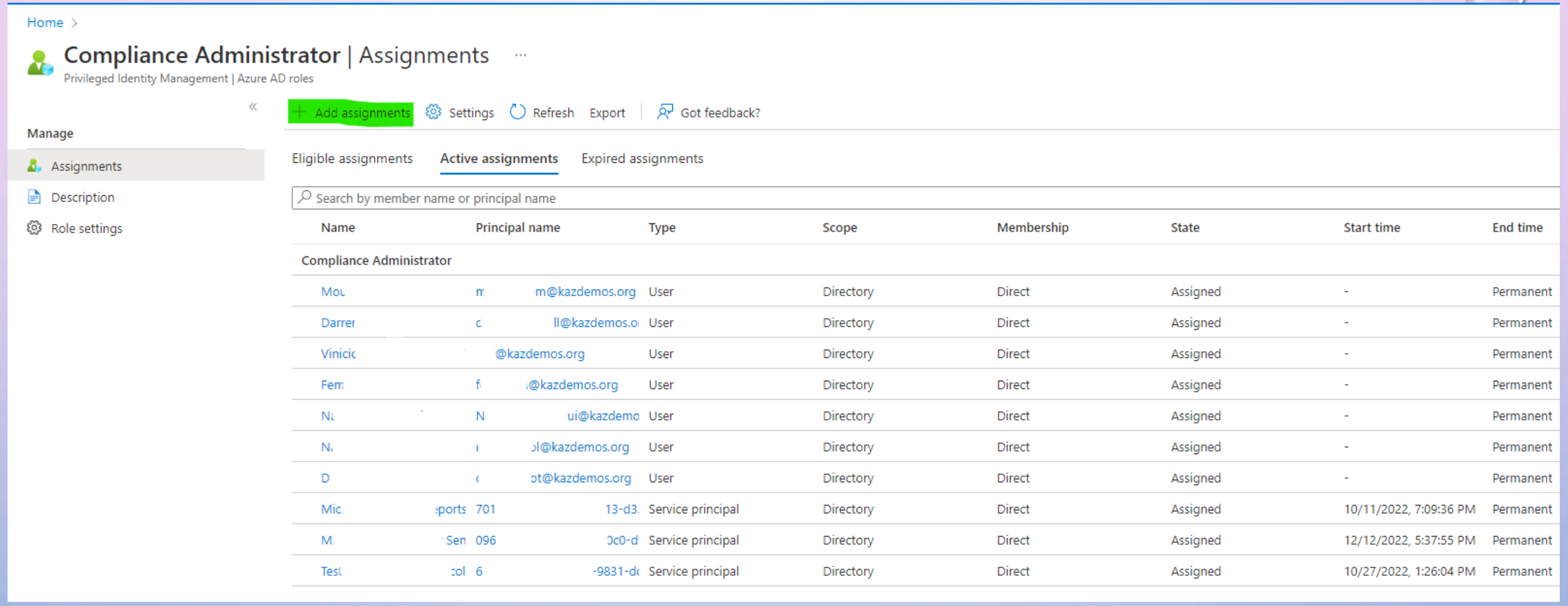
STEPS



Microsoft

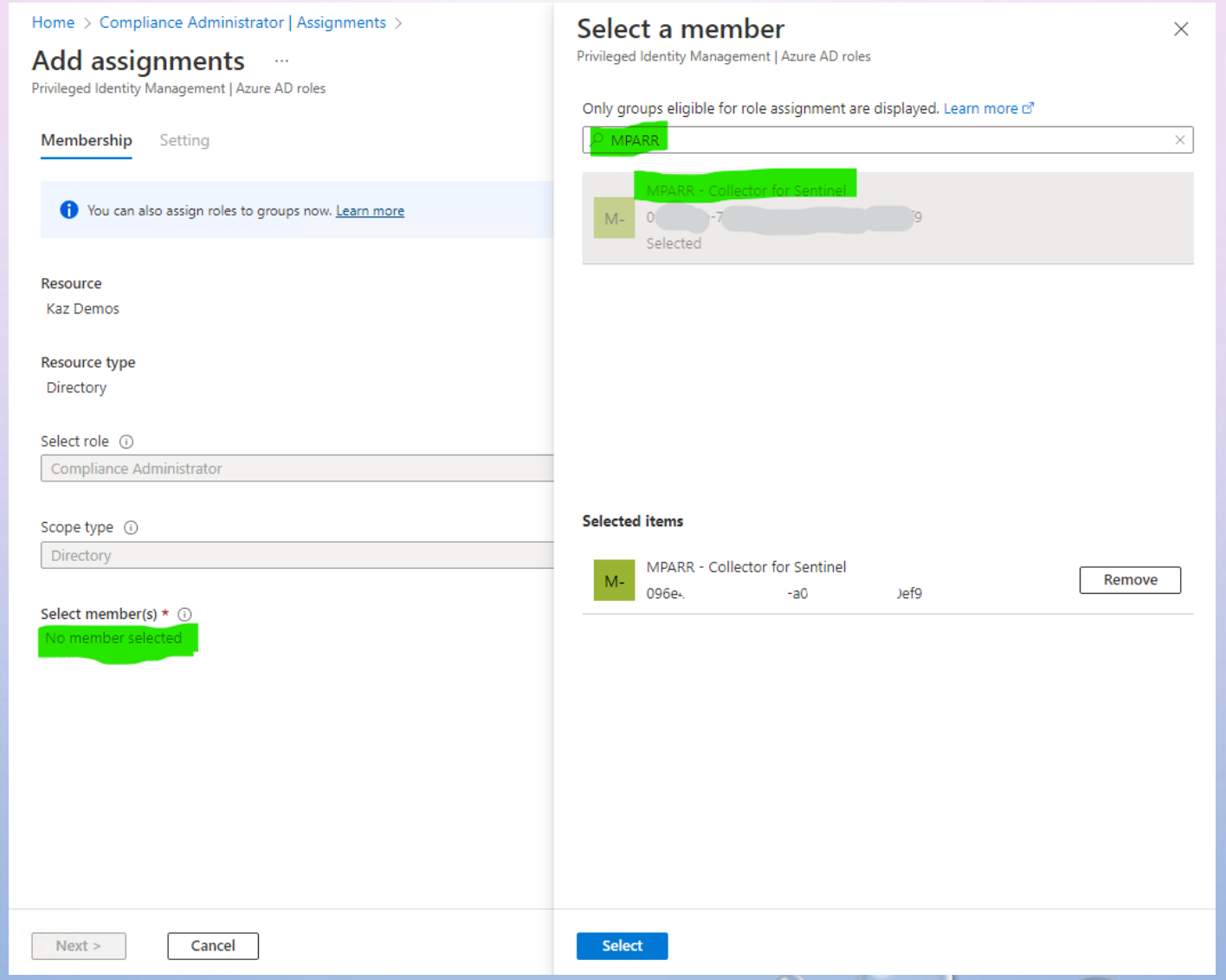
COMPLIANCE ADMIN ROLE FOR SCRIPT

STEPS



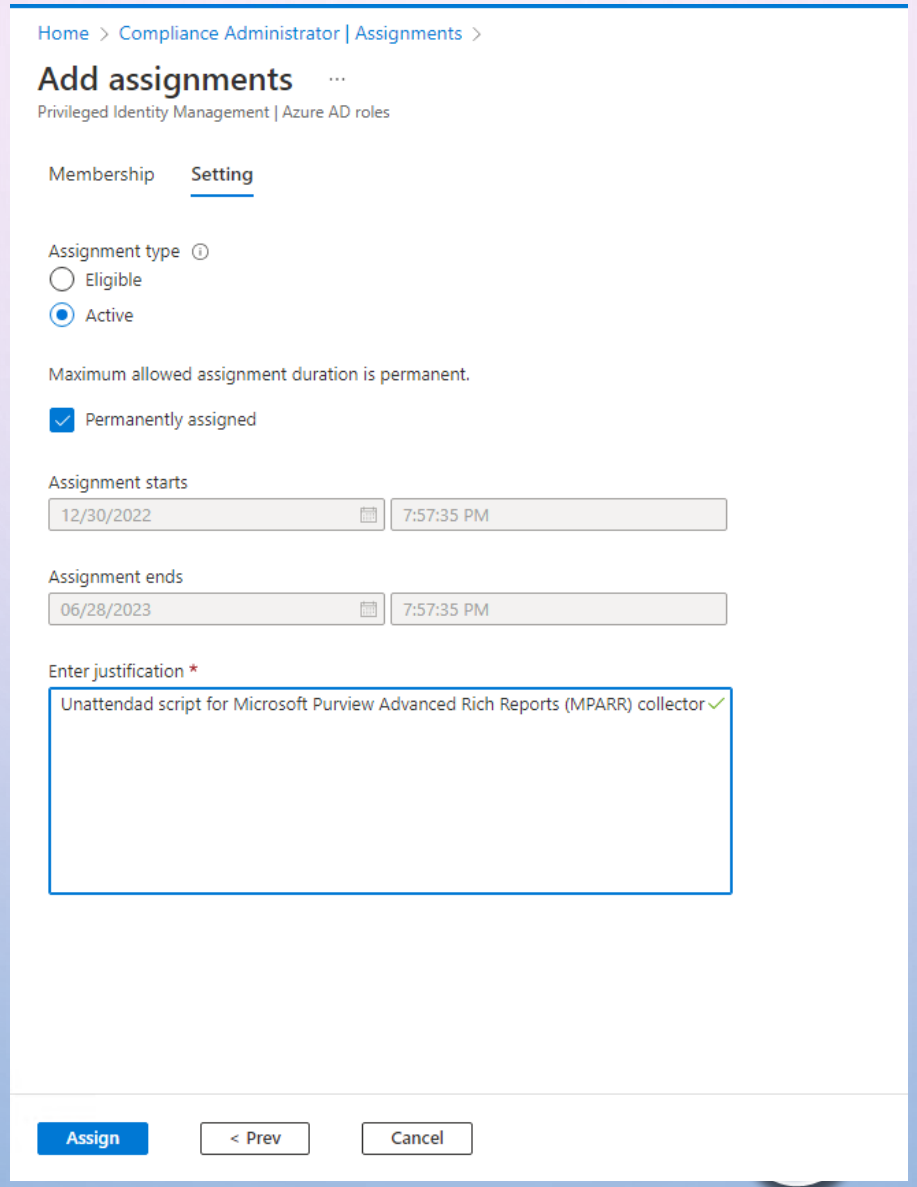
COMPLIANCE ADMIN ROLE FOR SCRIPT

STEPS



COMPLIANCE ADMIN ROLE FOR SCRIPT

STEPS



Microsoft

WORKSTATION OR SERVER

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

Microsoft

WORKSTATION OR SERVER

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

Microsoft

WORKSTATION OR SERVER

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*

Microsoft

WORKSTATION OR SERVER

STEPS

```
{
    "EncryptedKeys": "False",
    "AppClientID": "7(      :f-2. .5-4  f-8  .3-c          20",
    "ClientSecretValue": "i5o                                  jRZEVbKs",
    "TenantGUID": "a       3-7  e-4  8-a  9-9          :2c",
    "TenantDomain": "kazdemos.org",
    "LA_CustomerID":  "5     d4c-7]  :-4:  d-8  :f-(          )4",
    "LA_SharedKey":  "kN                                 HDKC                                                    )l4dw==",
    "Cloud": "Commercial",
    "CertificateThumb": "18                                                    0F4179BCD9",
    "OnmicrosoftURL": "M3          .onmicrosoft.com",
    "RMSLogs": "c:\\Collector\\Script2.0\\RMSLogs\\",
    "OutPutLogs": "Logs\\"
}
```

Microsoft

WORKSTATION OR SERVER

STEPS

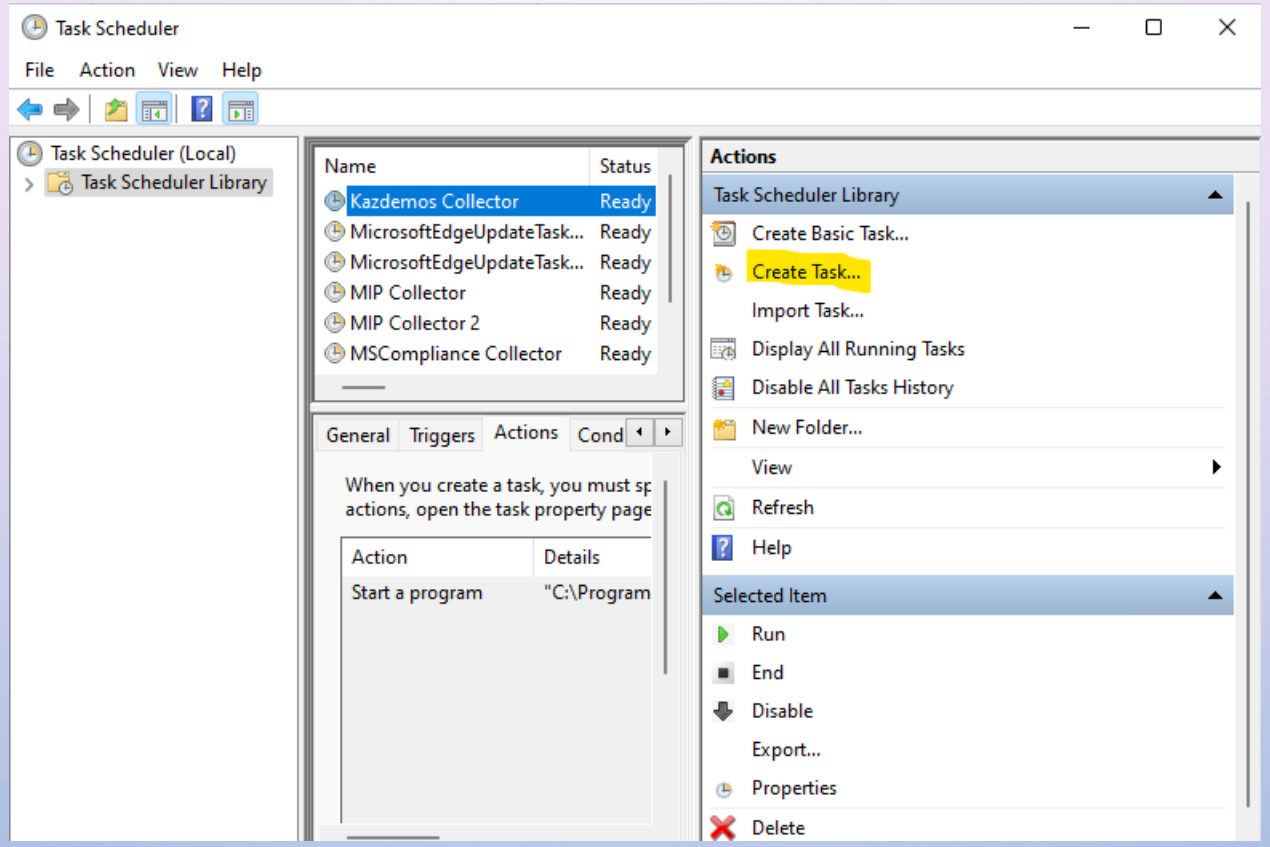
run_me.ps1 | Get-AzureADData.ps1 | schemas.json | Get-LabelData.ps1 | Get-RMSData.ps1 | Get-RMSData.ps1

```
{
    "Audit.AzureActiveDirectory": "True",
    "Audit.Exchange": "True",
    "Audit.SharePoint": "True",
    "Audit.General": "True",
    "DLP.All": "True"
}
```

Microsoft

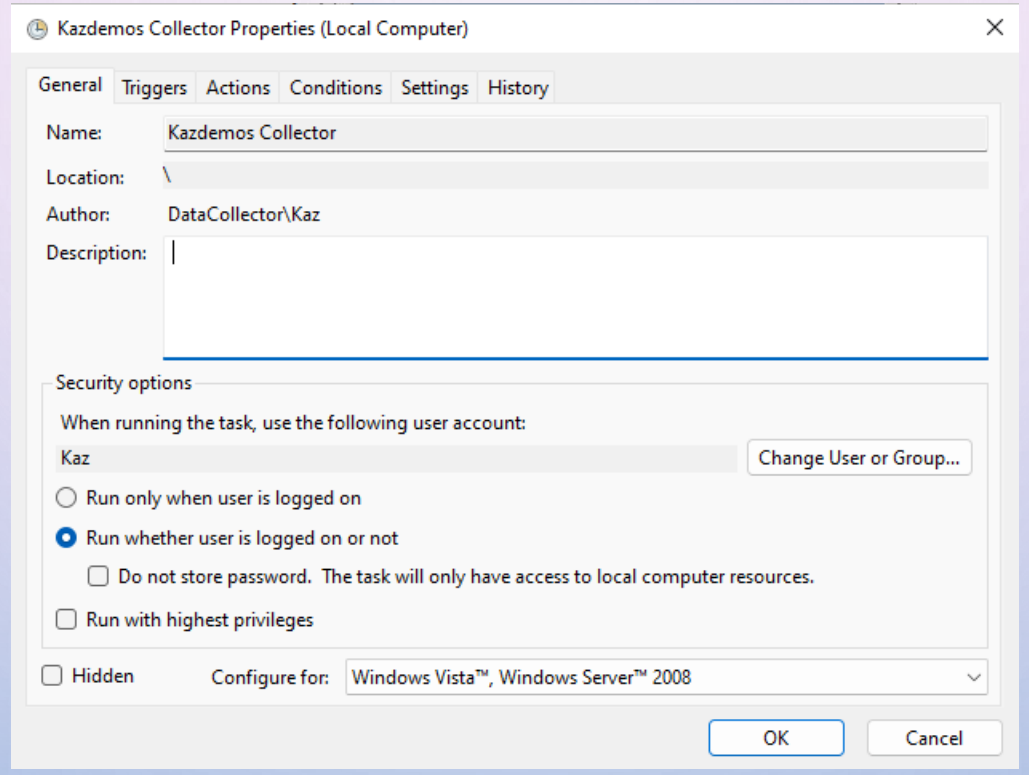
WORKSTATION OR SERVER

STEPS



WORKSTATION OR SERVER

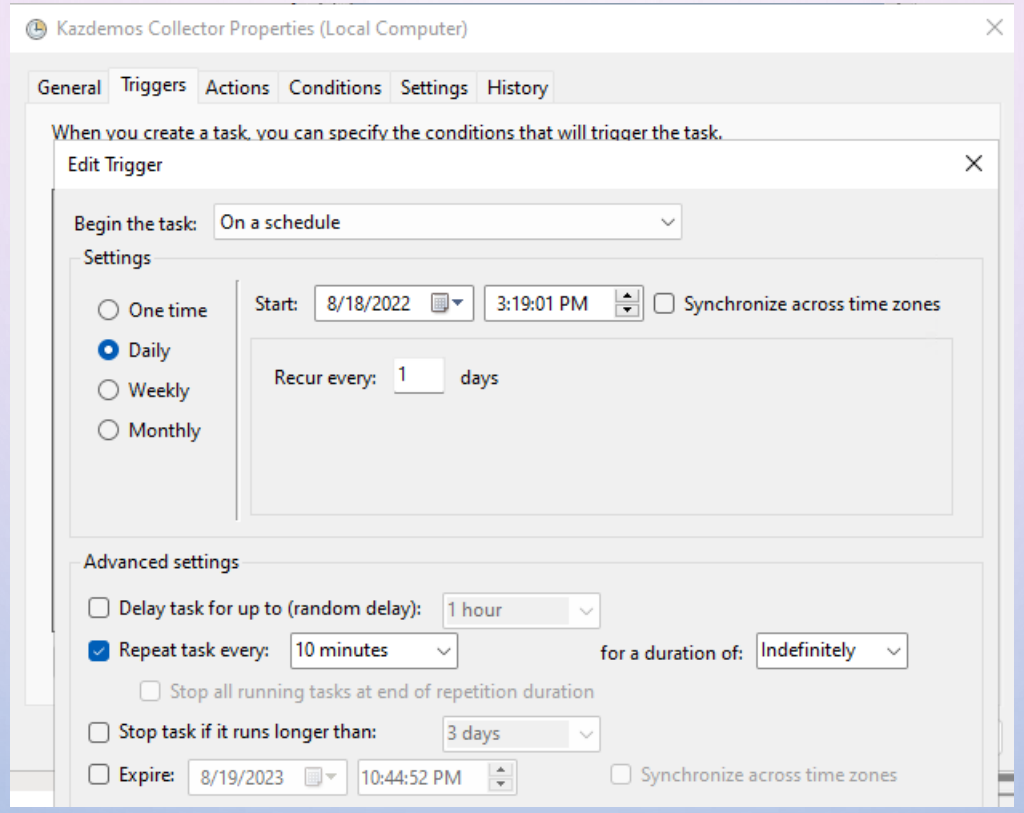
STEPS



Microsoft

WORKSTATION OR SERVER

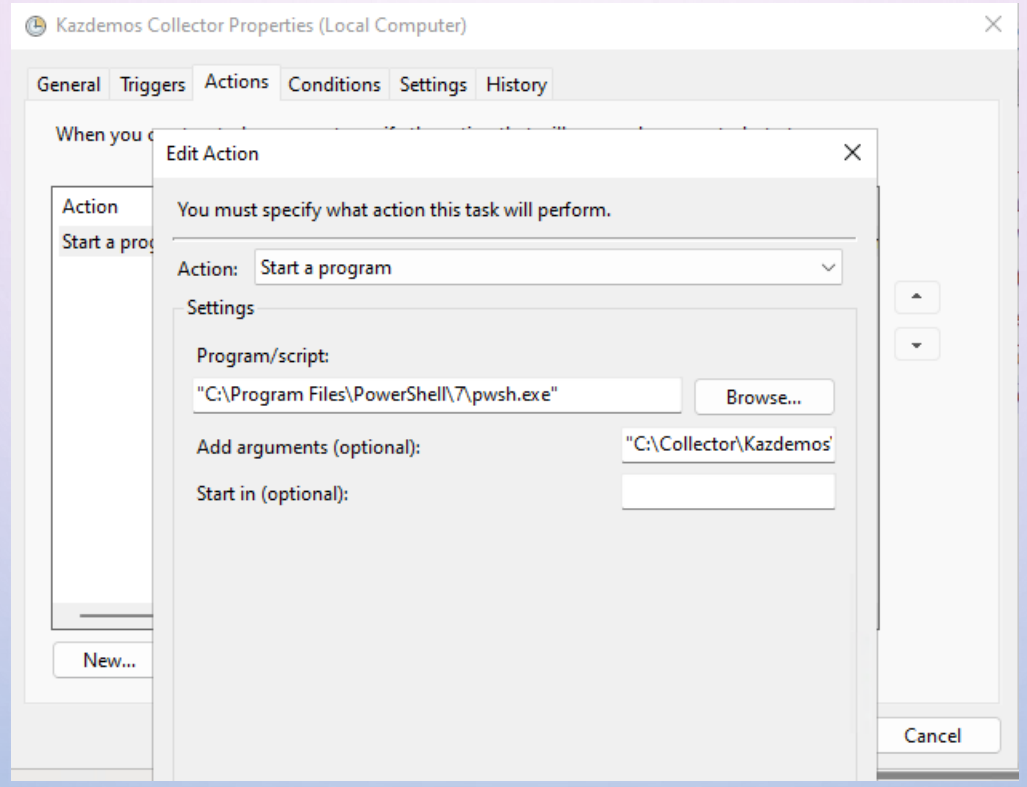
STEPS



Microsoft

WORKSTATION OR SERVER

STEPS

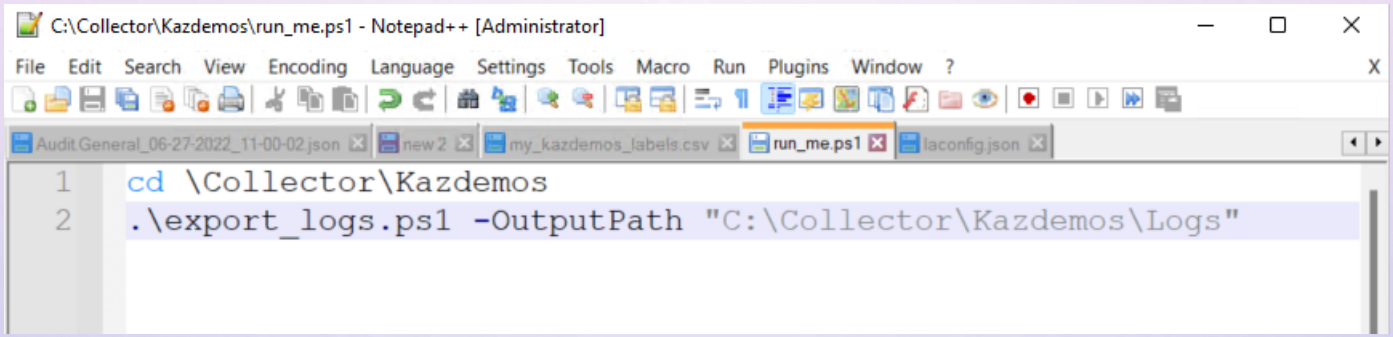


Microsoft

WORKSTATION OR SERVER

TO EXECUTE THE SCRIPT WITH PARAMETERS

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



- 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

Microsoft

WORKSTATION OR SERVER

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:

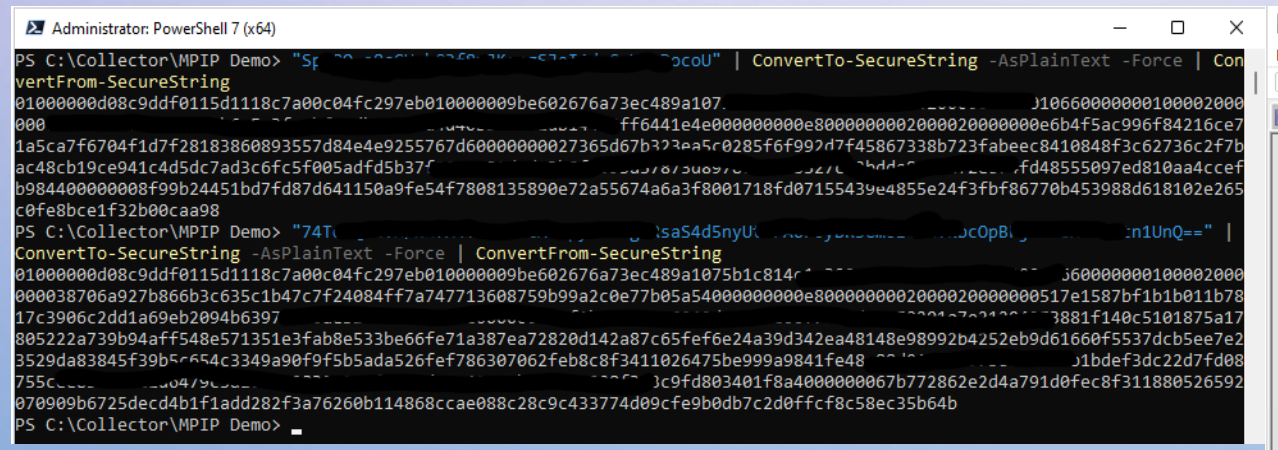
- `PS C:\> "CLIENTSECRETVALUE**" | CONVERTTO-SECURESTRING -ASPLAINTEXT -FORCE | CONVERTFROM-SECURESTRING`
- **REPLACE THE VALUE ON LACONFIG.JSON WITH THE NEW STRING**

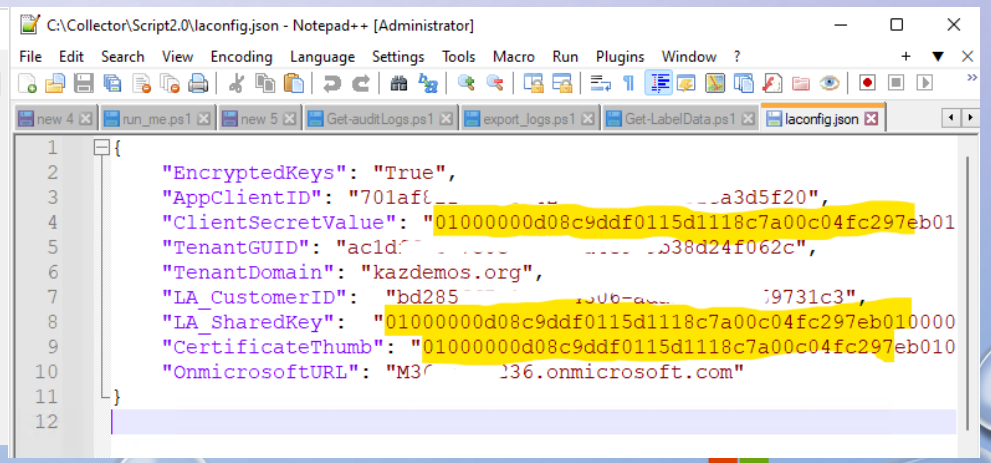
COPY THE VALUE FOR "LA_SHAREDKEY" AND EXECUTE ON POWERSHELL THIS CMDLET:

- `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**





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

***Use the key value*

SELECT TENANT TYPE

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

Microsoft

MS PURVIEW - POWERSHELL

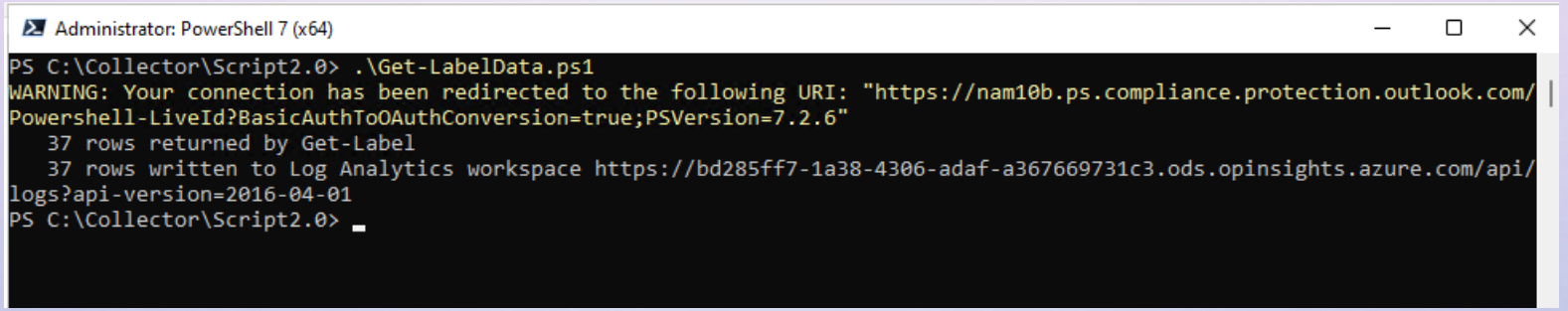
OBTAIN YOUR LABEL LIST WITH IDS AND SEND TO LOGS ANALYTICS

- 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 1ST.
- 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.

**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*

WORKSTATION - POWERSHELL

STEPS



Microsoft

SERVICE PLAN IDENTIFIERS FOR LICENSING

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.PS1YOU 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"
```

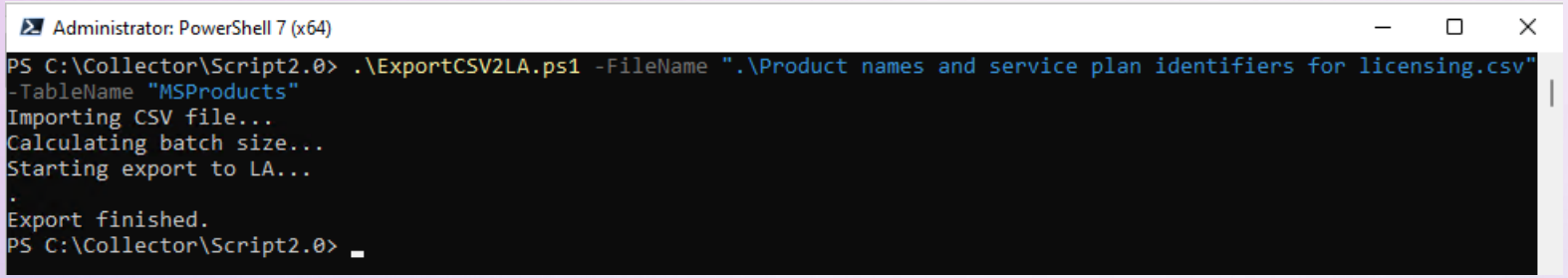
- AFTER EXECUTING THE SCRIPT CAN TAKE BETWEEN 5 TO 10 MINUTES TO DISPLAY THE NEW TABLE UNDER LOGS ANALYTICS
- HOW TO CONSUME THROUGH POWER BI, CLICK HERE.

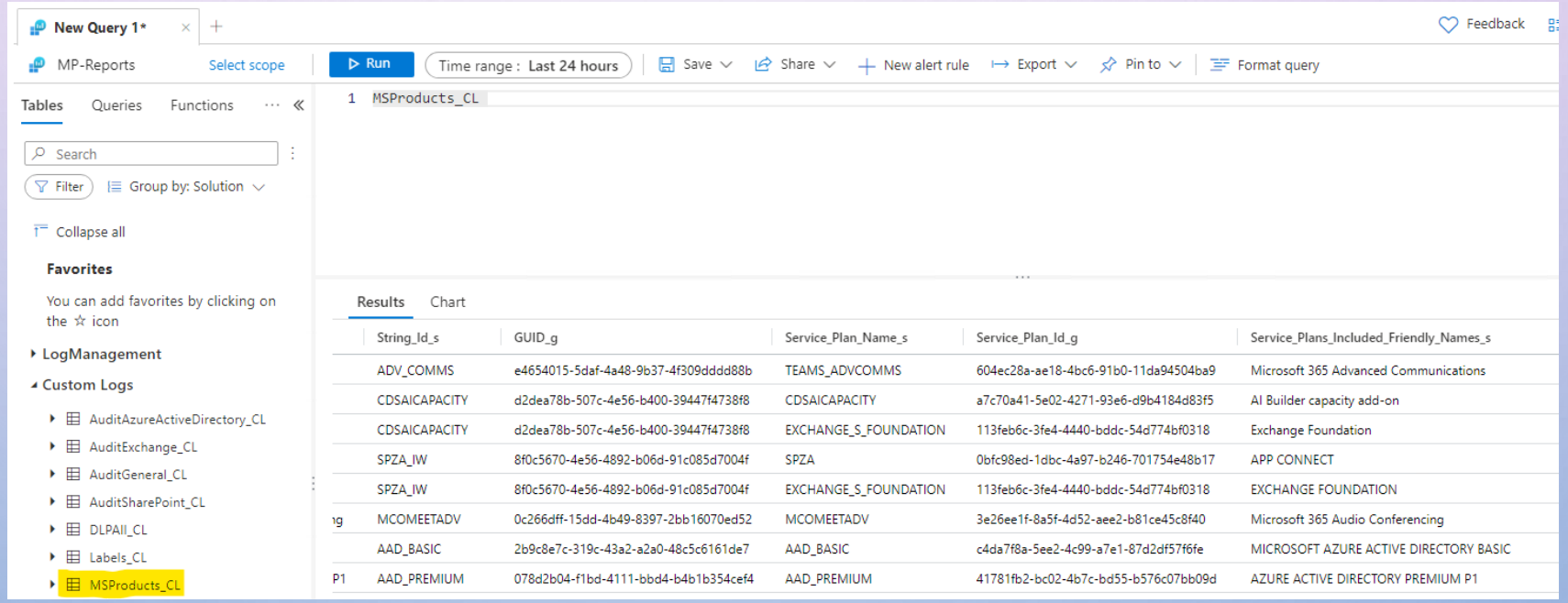
*https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-service-plan-reference
**Depending on the Logs Analytics workspace retention this script will be required to execute continuously(monthly for a 30 days retention period) to don't lose that information
*** Power BI templates use the table name called "MSProducts" any change to this name, need to make the change on Power BI queries

Microsoft

IMPORT DATA TO LOGS ANALYTICS

STEPS





LIST OF AZURE AD USERS WITH ATTRIBUTES AND LICENSING

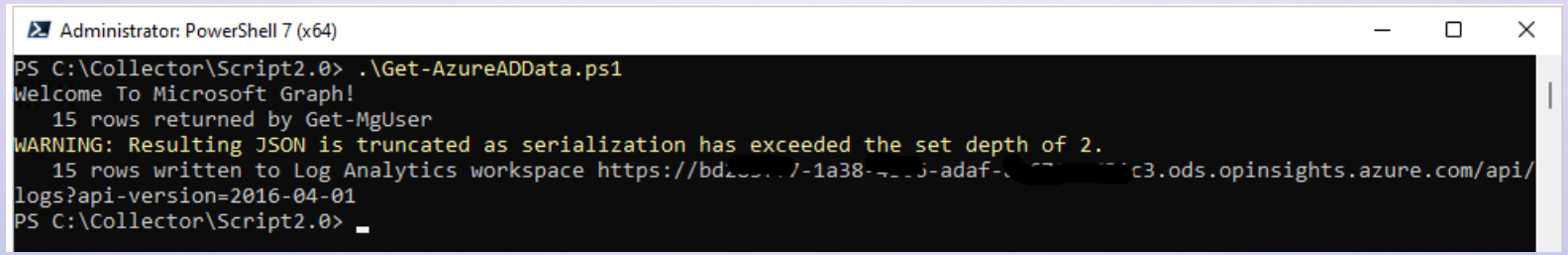
- PLEASE COMPLETE FIRST ALL THIS STEPS, **MICROSOFT GRAPH API** IS USED TO OBTAIN THE NEXT INFORMATION
- TO GENERATE A LIST OF AZURE AD USERS WITH SOME ATTRIBUTES LIKE COUNTRY, CITY, DEPARTMENT, JOB TITLE, OR OFFICE LOCATION, YOU NEED EXECUTE THE SCRIPT **GET-AZUREADDATA.PS1** PREVIOUSLY CHECK THAT YOU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

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

**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*

POWERSHELL - AZURE AD USERS

STEPS



LIST OF AZURE AD ROLES AND DOMAINS REGISTERED

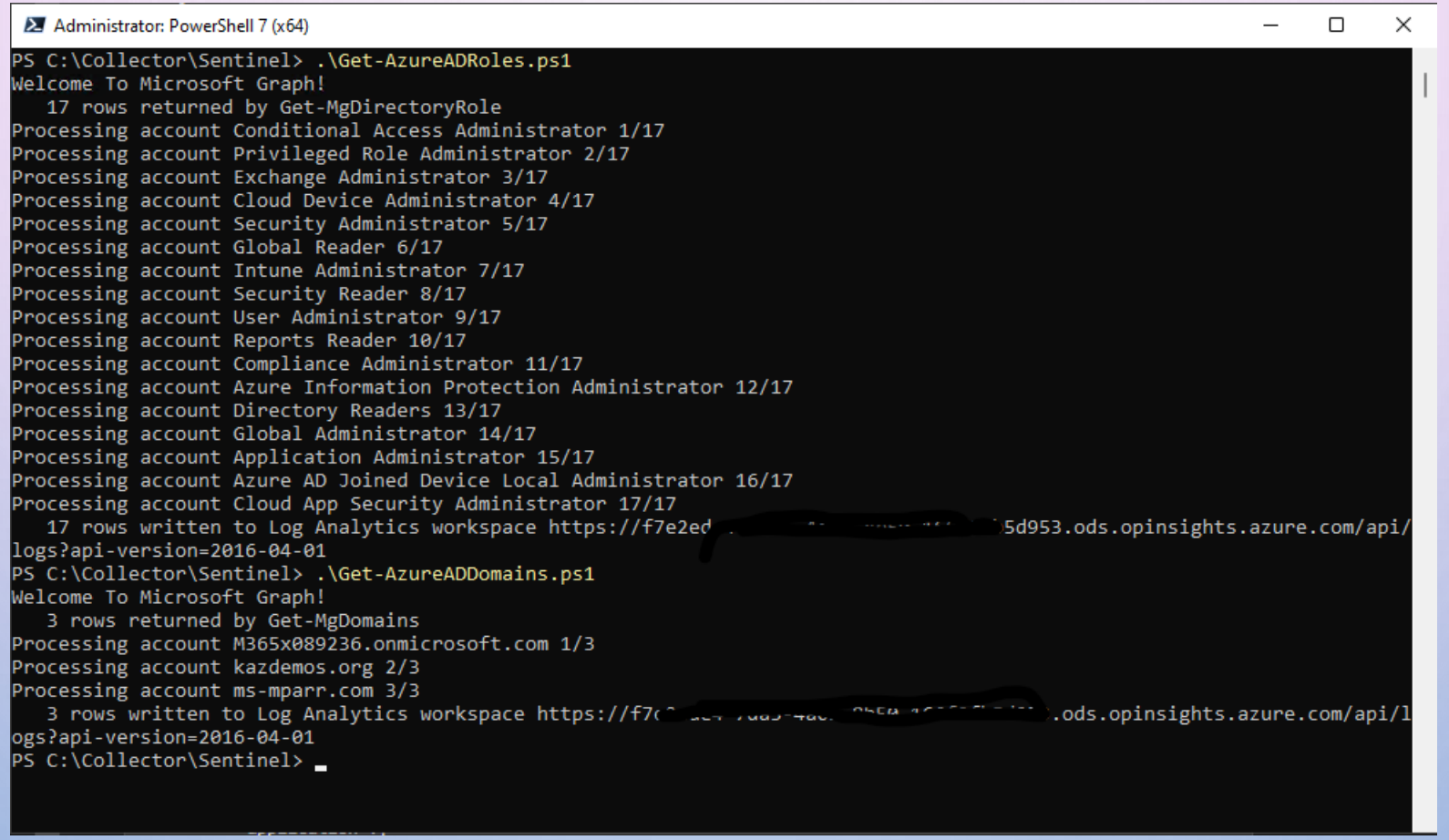
- PLEASE COMPLETE FIRST ALL THIS STEPS, **MICROSOFT GRAPH API** IS USED TO OBTAIN THE NEXT INFORMATION
- TO GENERATE A LIST OF AZURE AD ROLES, AND DOMAINS REGISTERED ON THE TENANT, YOU NEED EXECUTE THE SCRIPT **GET-AZUREADROLES.PS1** AND **GET-AZUREADDOMAINS.PS1,** PREVIOUSLY CHECK THAT YOU ARE USING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

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

**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*

POWERSHELL - AZURE AD USERS

STEPS



CONNECT TO LOGS STORED IN YOUR WORKSPACE

- OPEN 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:
    - **AUDITAZUREACTIVEDIRECTORY_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

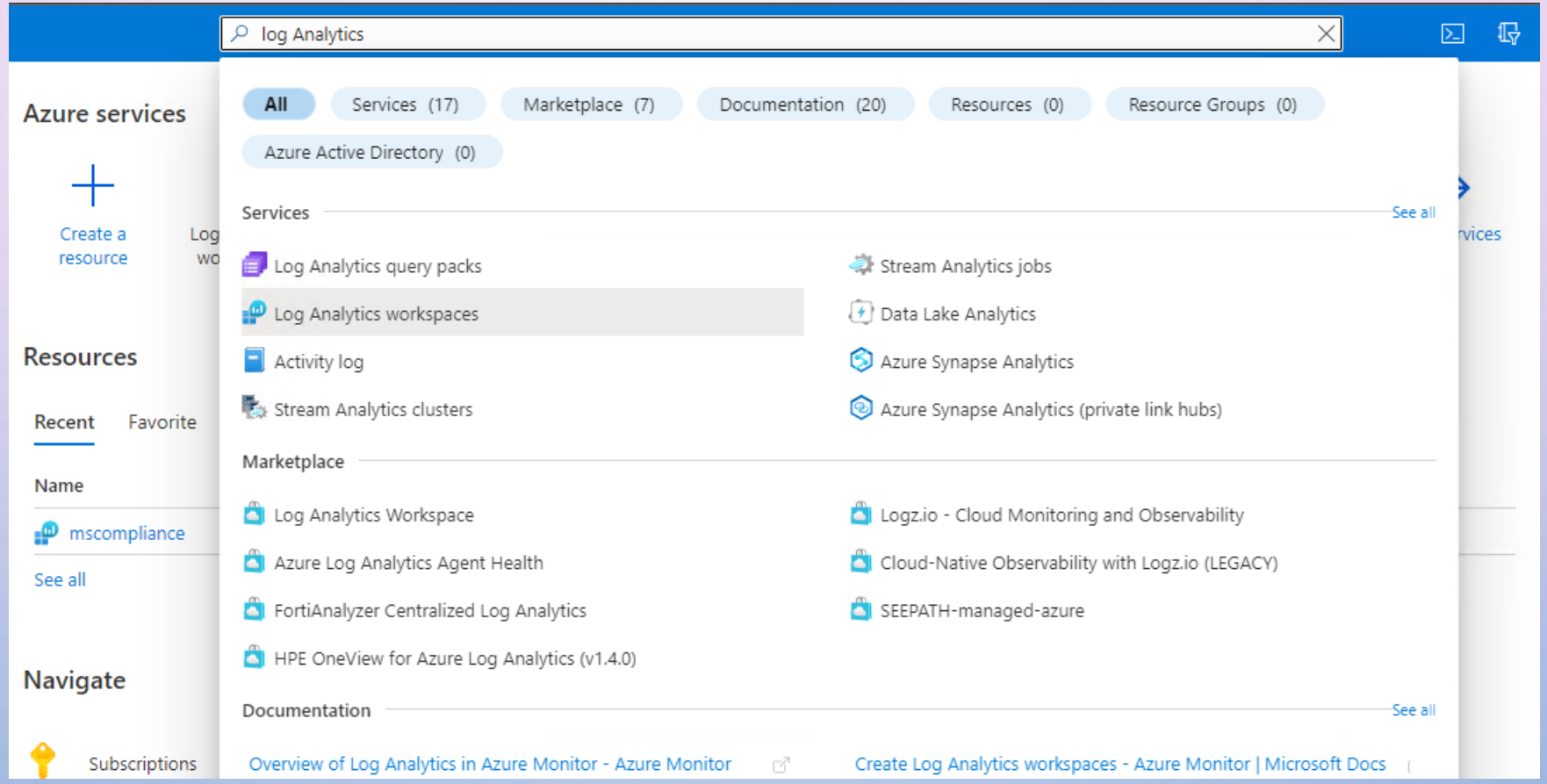
- THE NEXT STEPS ARE REQUIRED TO DO FOR EACH TABLE (5):
  - DOUBLE CLICK IN TABLE NAME, THAT ACTION WILL BE PUT THE NAME OF THE TABLE ON QUERY SPACE
  - PRESS RUN BUTTON (IS NOT REQUIRE MAKE CHANGES OVER TIME RANGE)
  - AFTER PRESSING THE QUERY WILL BE RUNNING AND SOME RESULTS WILL BE APPEARED AT RESULT 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.

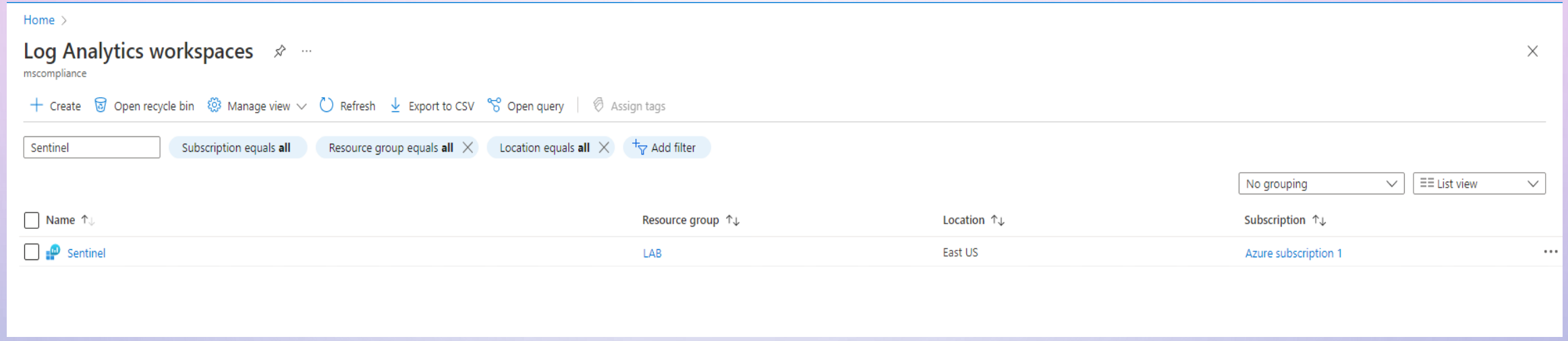
LOGS ANALYTICS WORKSPACE

STEPS



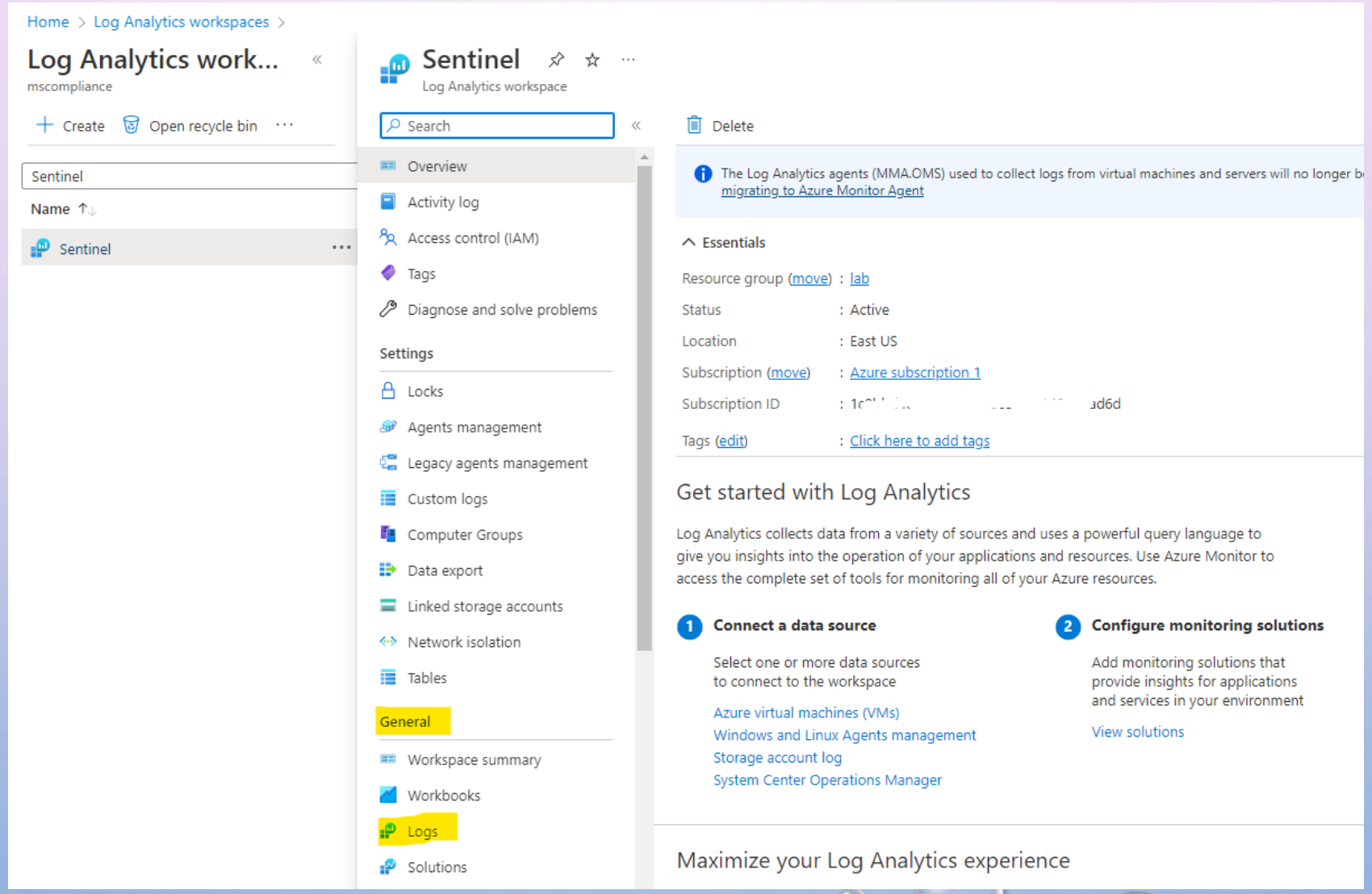
LOGS ANALYTICS WORKSPACE

STEPS



LOGS ANALYTICS WORKSPACE

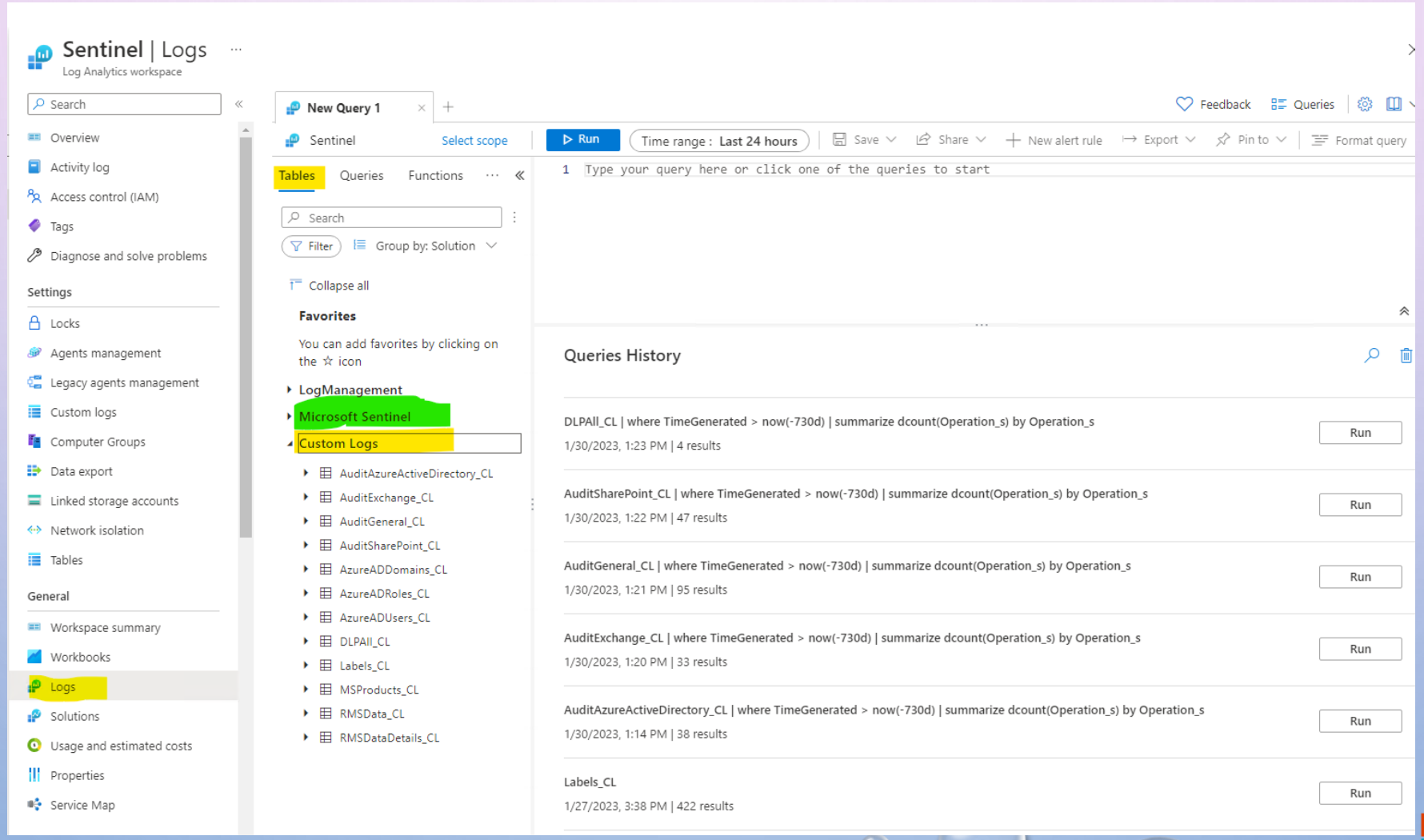
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

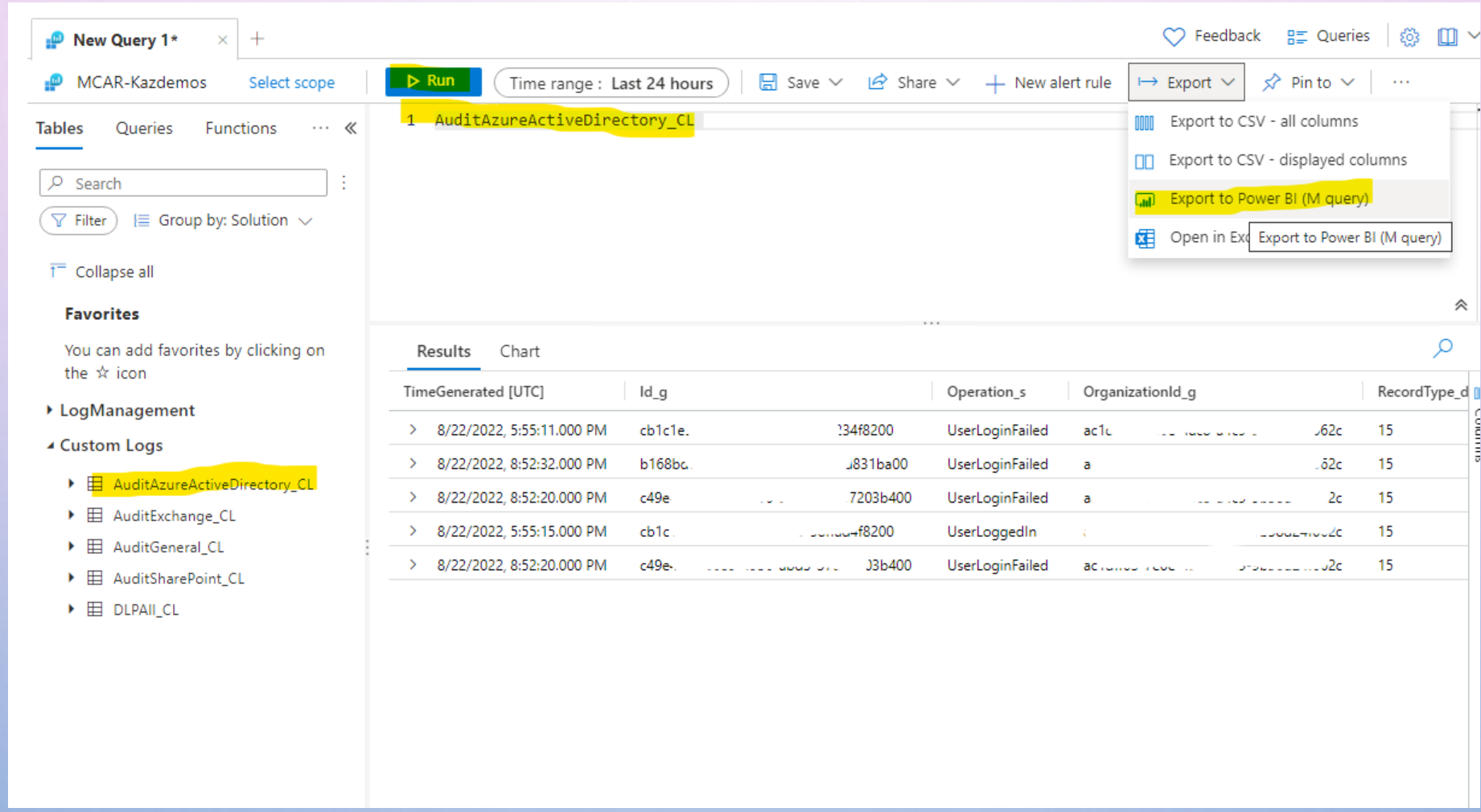
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

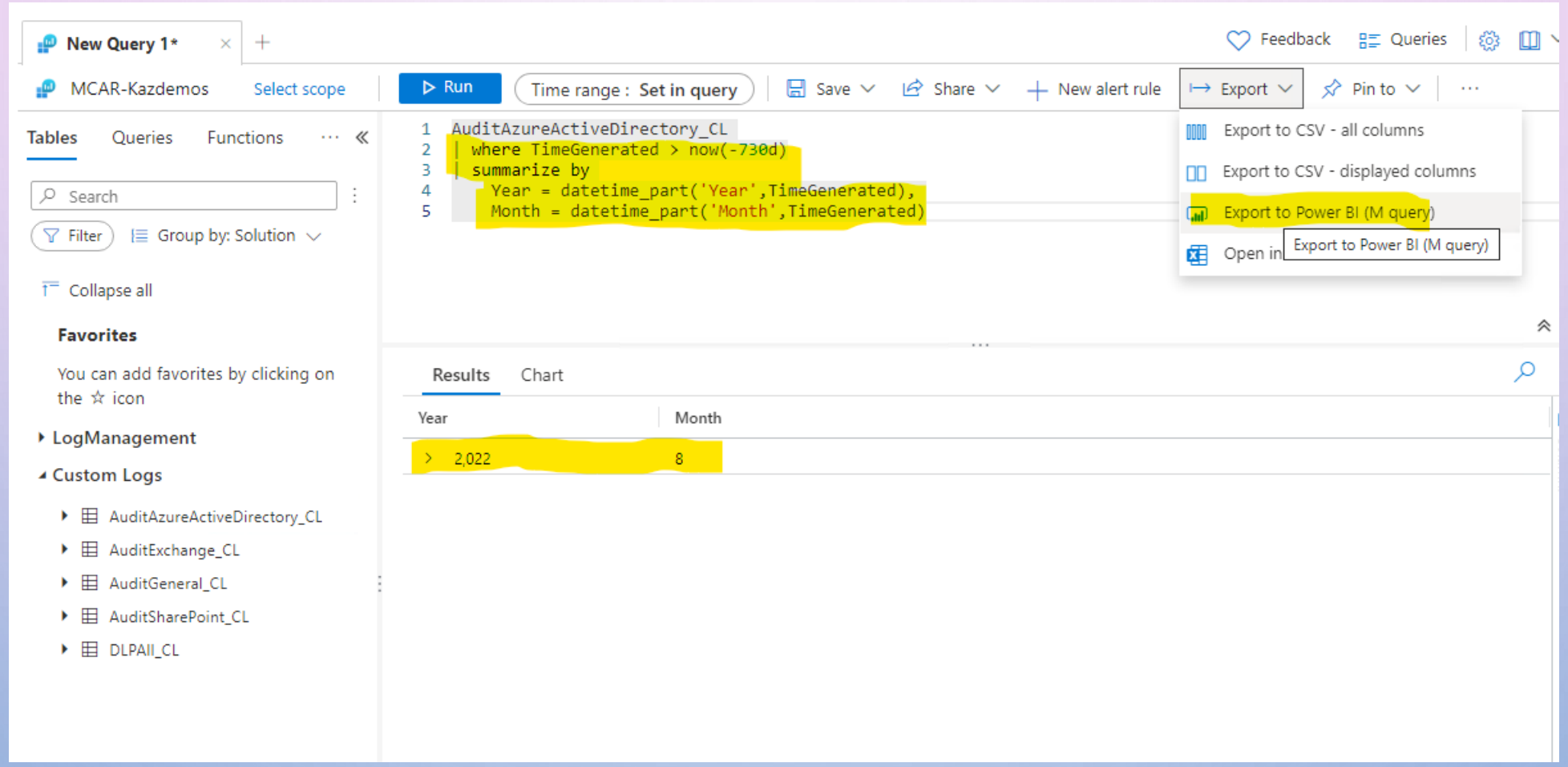
STEPS



Microsoft

LOGS ANALYTICS WORKSPACE

STEPS



LOGS ANALYTICS WORKSPACE

EXPORT EXAMPLE

File Edit View

```
/*
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

Microsoft

KQL FOR LATEST LABEL INFORMATION

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

Microsoft

KQL FOR LATEST INFORMATION

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

Microsoft

KQL FOR LATEST AZURE AD INFORMATION

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

Microsoft

POWER BI

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

Microsoft

POWER BI

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.

Microsoft

POWER BI

POWER BI LIMIT RESOLVED

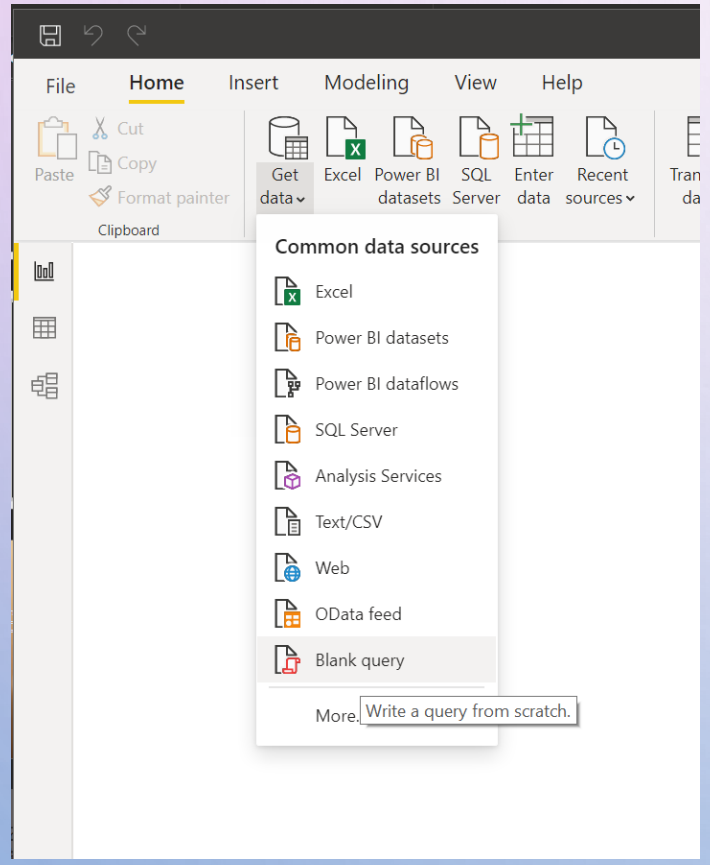
21. AFTER FINISH THE PREVIOUS STEPS WITH THE 5 TABLES IS REQUIRED MERGE THE QUERIES WITH THE FUNCTIONS, TO DO THAT PLEASE GO FORWARD WITH THE NEXT STEPS TAKING CARE IN EACH POINT
22. SELECT YOUR QUERY (THE ONE WITH YEAR AND MONTH AS RESULT), AT THE TOP SELECT THE TAB ADD COLUMN AND THEN PRESS INVOKE 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 COLUMNA NAME

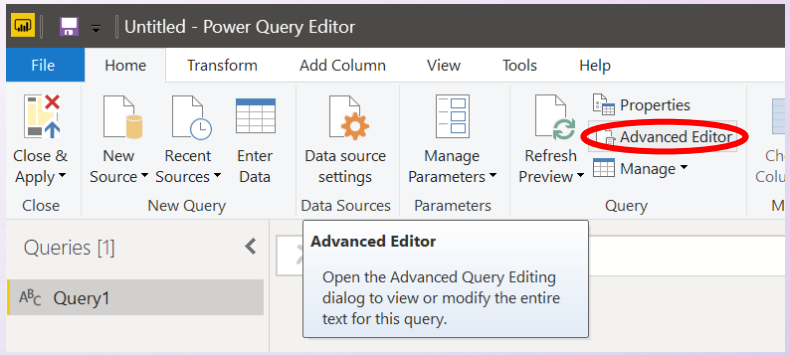
25. IN NEW WINDOW ALL COLUMNS RELATED TO THE ORIGINAL TABLE WILL BE APPEAR (SOMETIMES APPEAR AT BOTTOM AN OPTION TO LOAD MORE COLUMNS, IN THAT CASE PLEASE PRESS THAT OPTION) UNCHECK USE ORIGINAL NAME AS PREFIX
26. NOW ALL THE COLUMNS WILL BE ADDED BASED ON THE DATE, THAT STEP RESOLVE THE 500K LIMIT ON 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

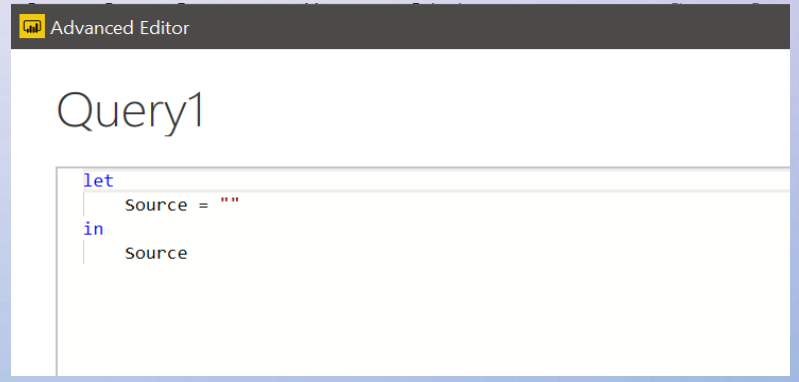
Microsoft

POWER BI

STEPS



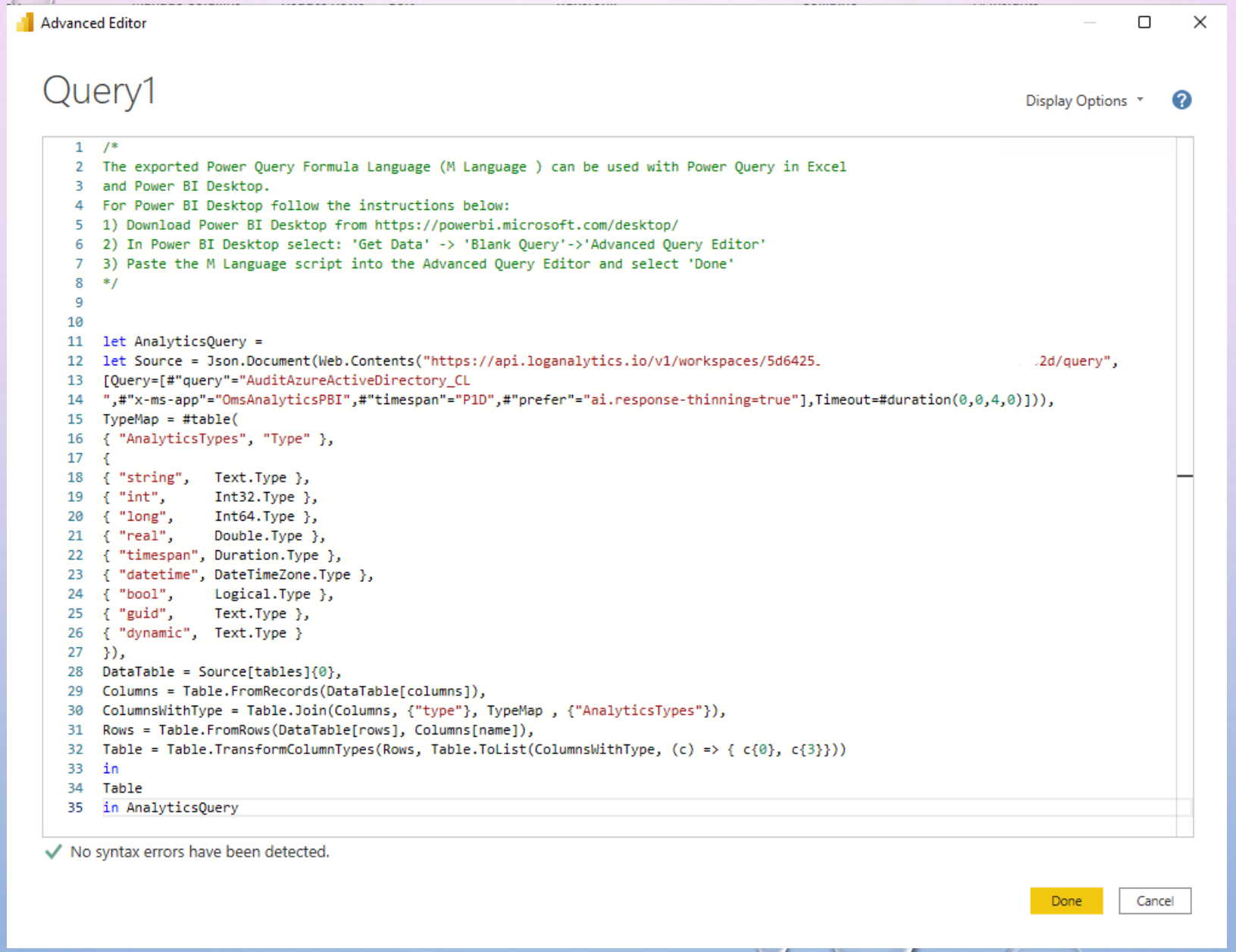




Microsoft

POWER BI

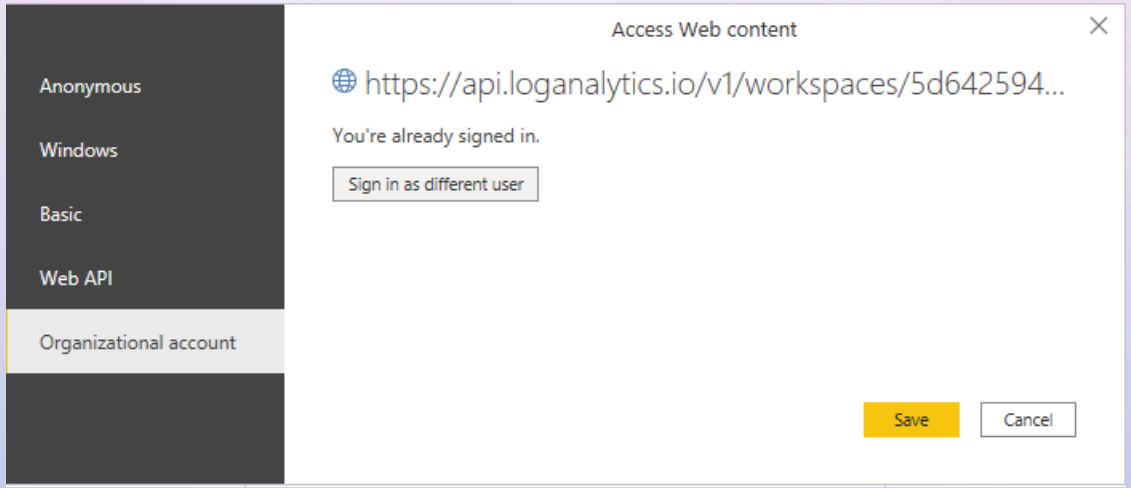
STEPS



Microsoft

POWER BI

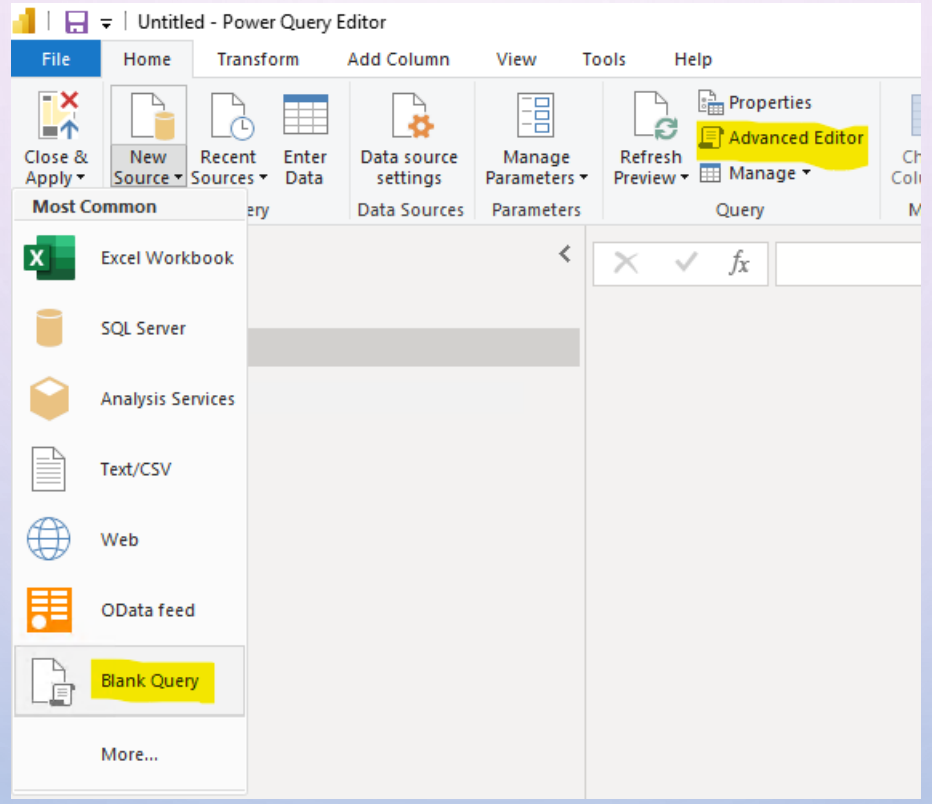
STEPS



Microsoft

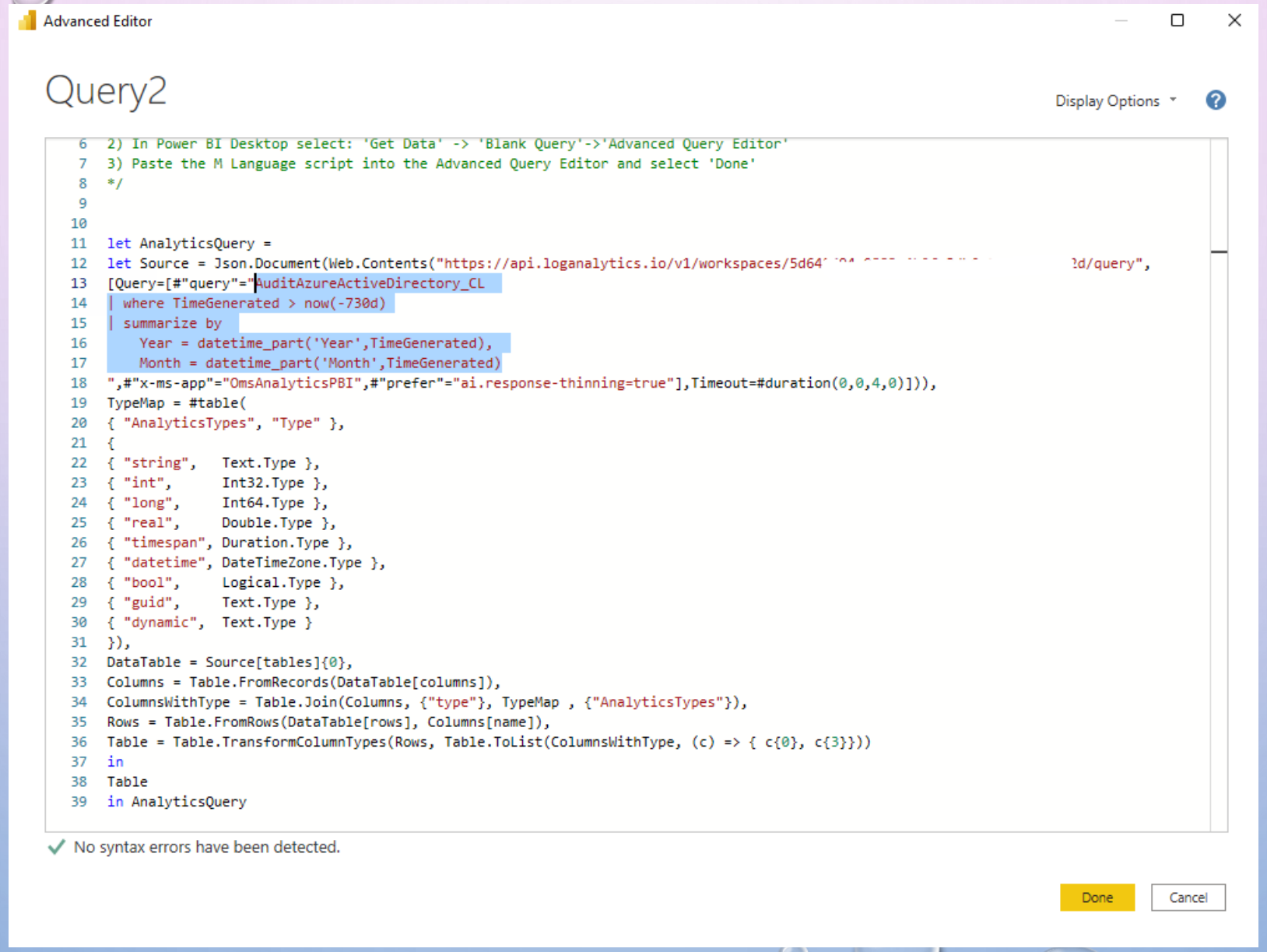
POWER BI

STEPS



POWER BI

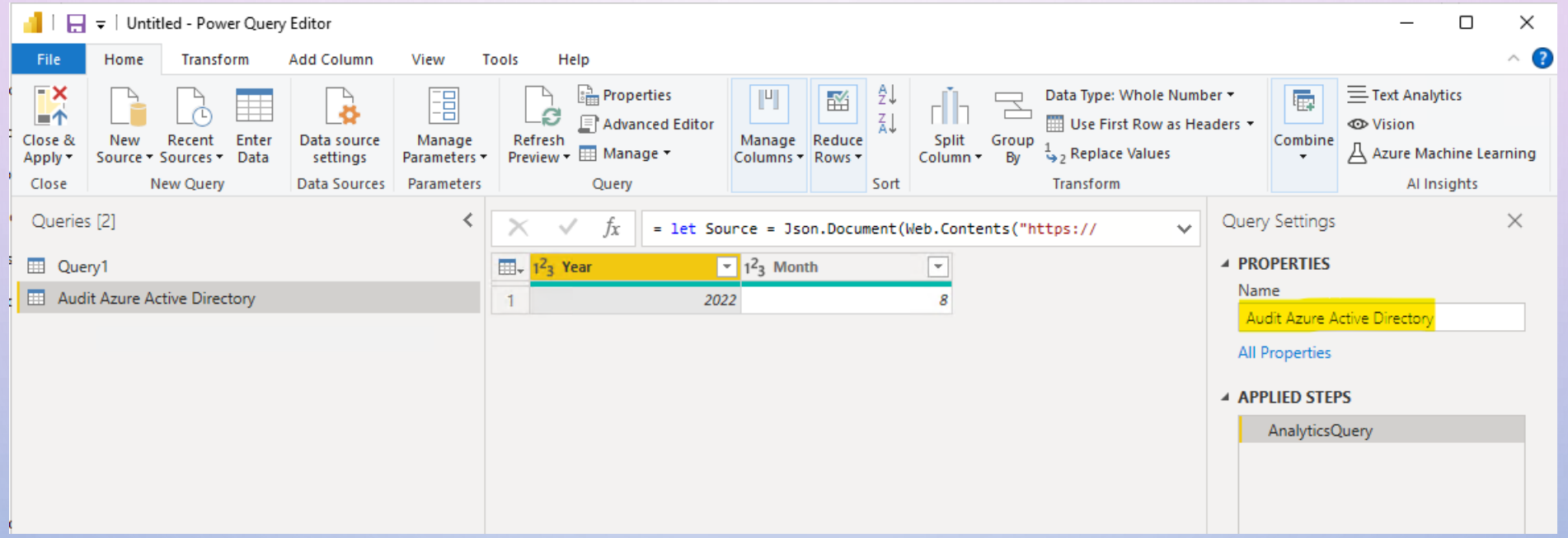
STEPS



Microsoft

POWER BI

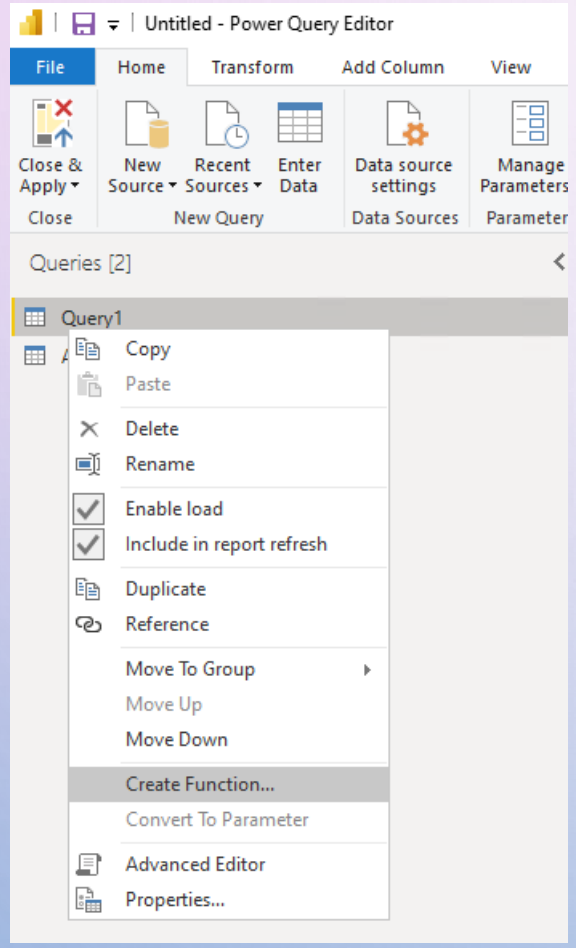
STEPS

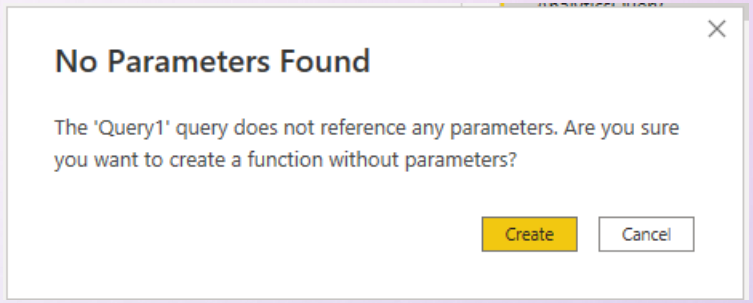


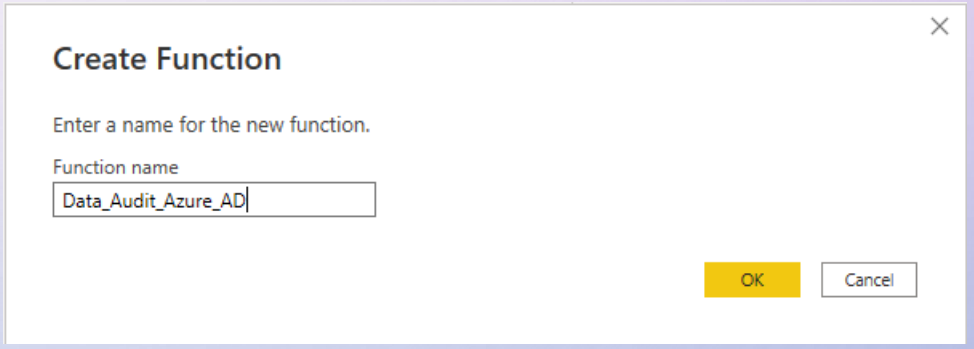
Microsoft

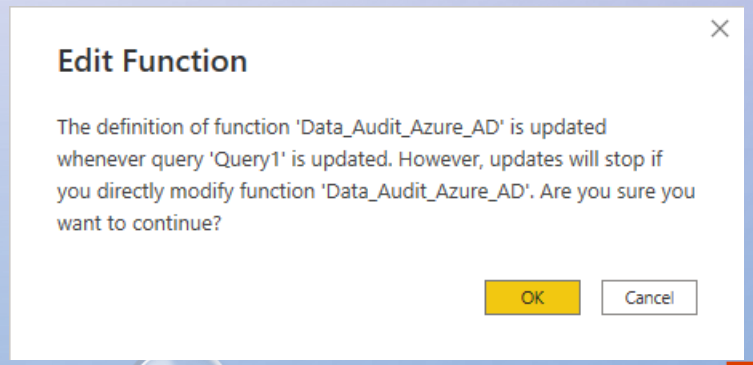
POWER BI

STEPS









Microsoft

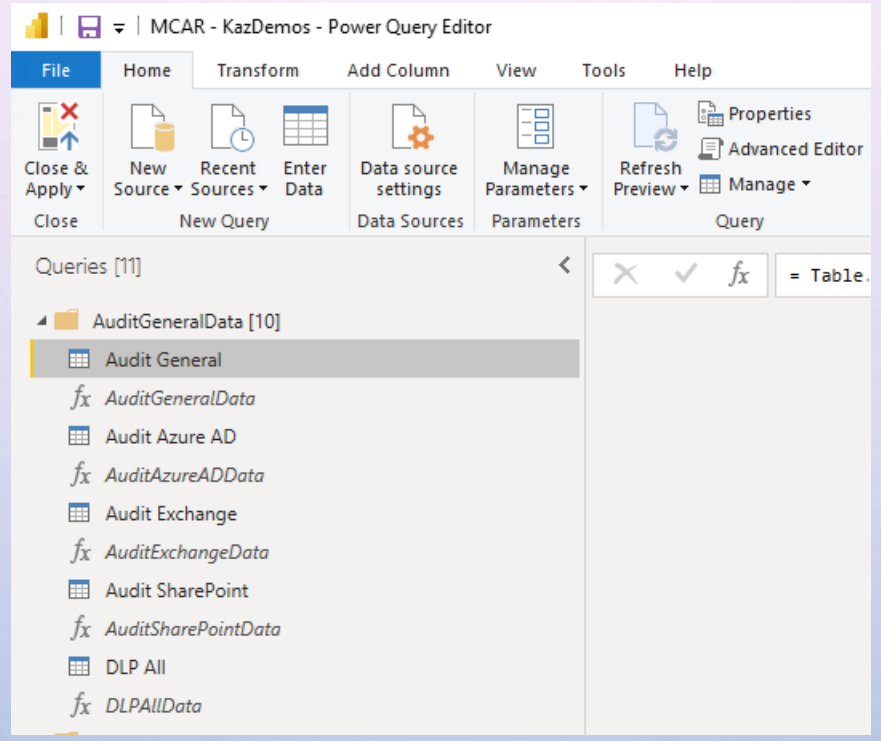
POWER BI

STEPS

Microsoft

POWER BI

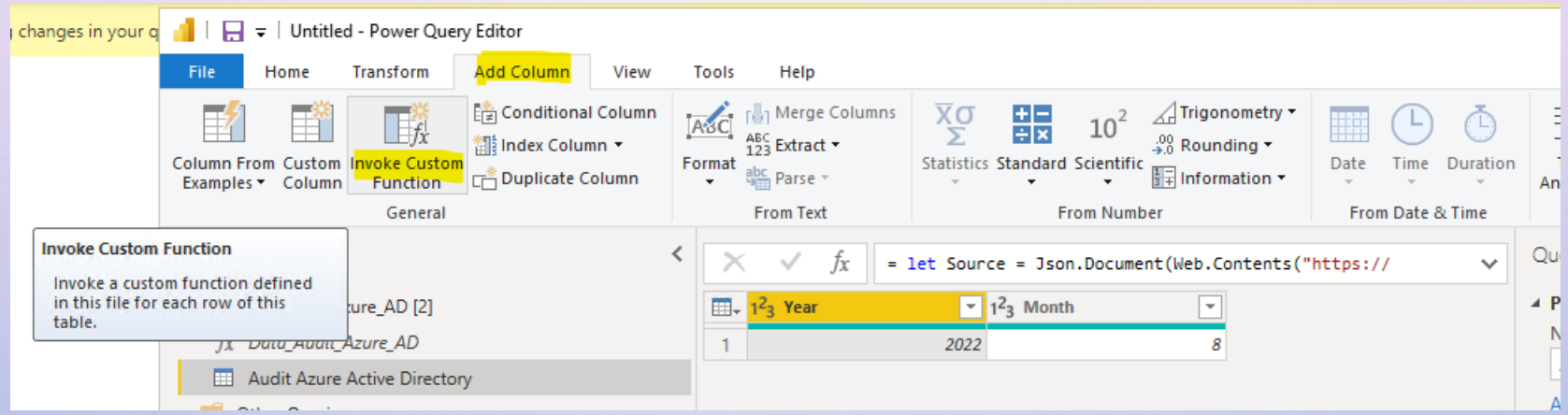
STEPS



Microsoft

POWER BI

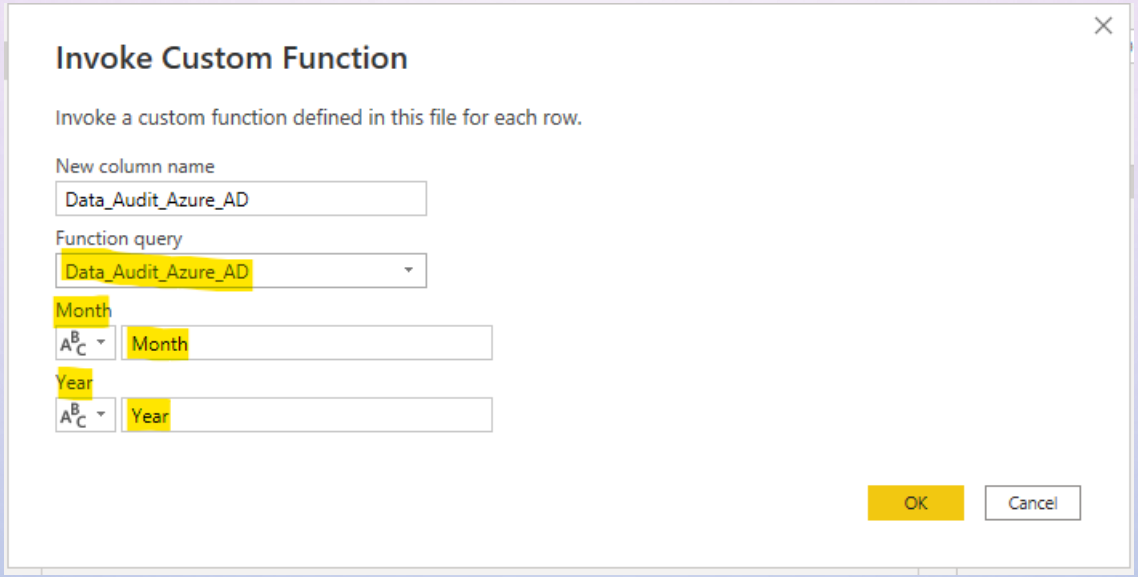
STEPS



Microsoft

POWER BI

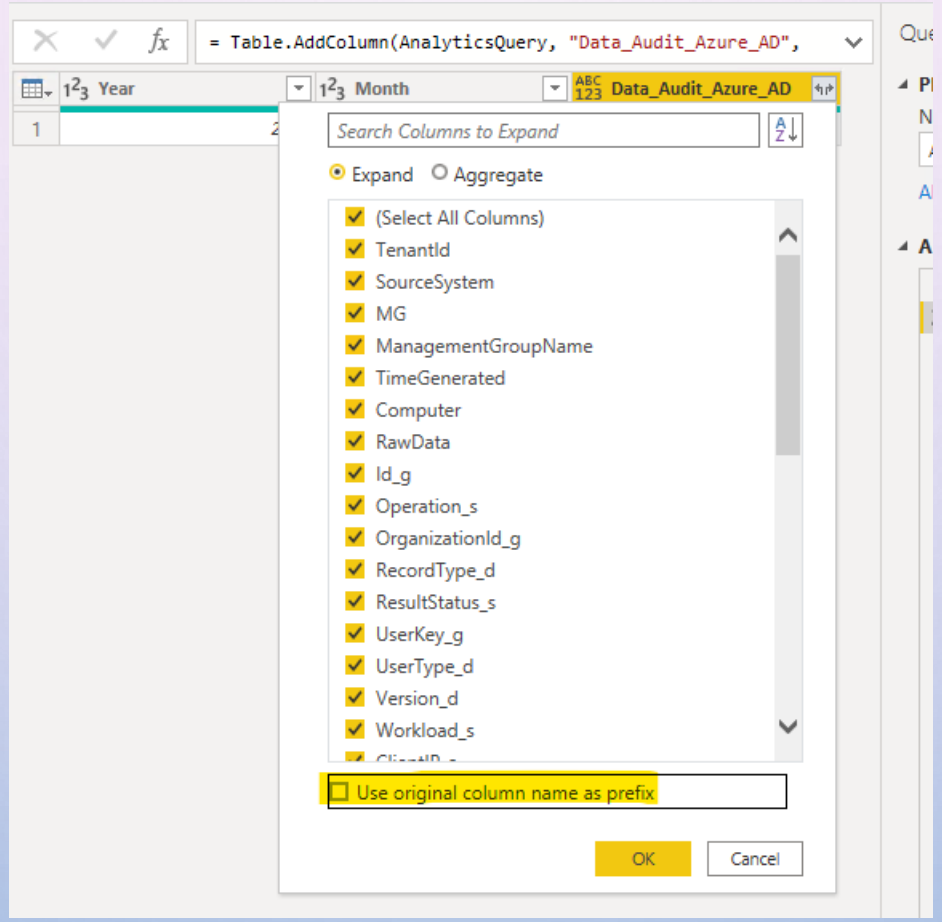
STEPS



Microsoft

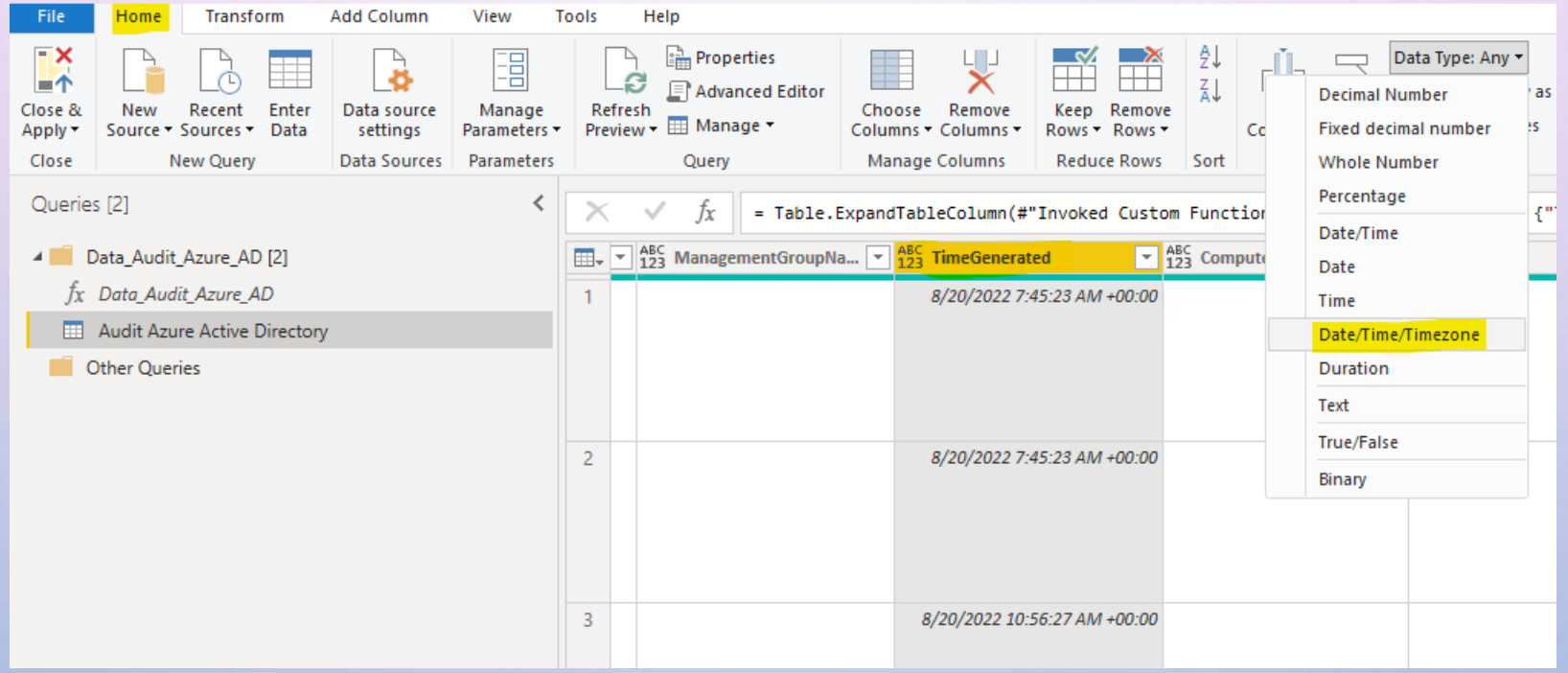
POWER BI

STEPS



POWER BI

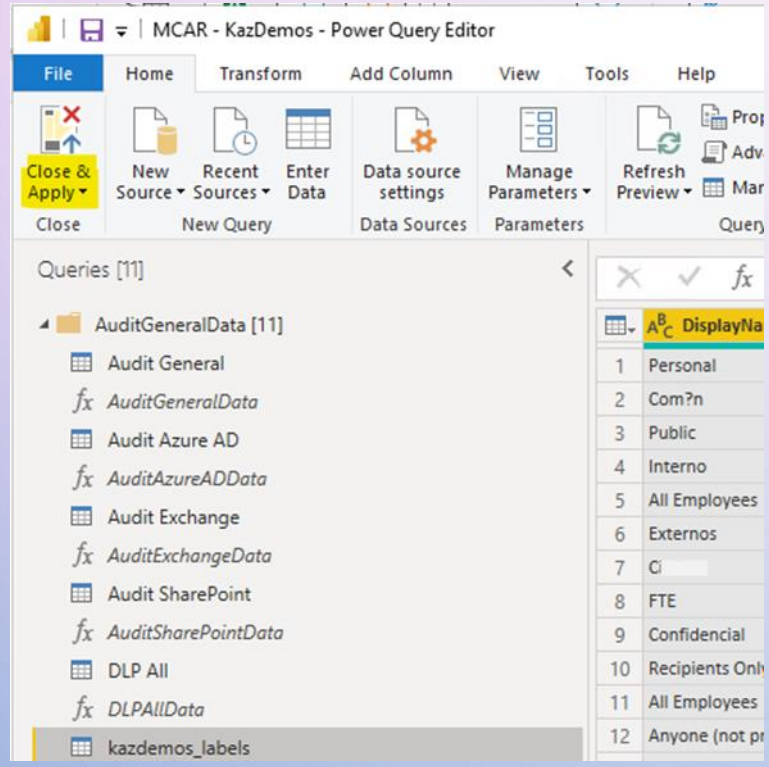
STEPS

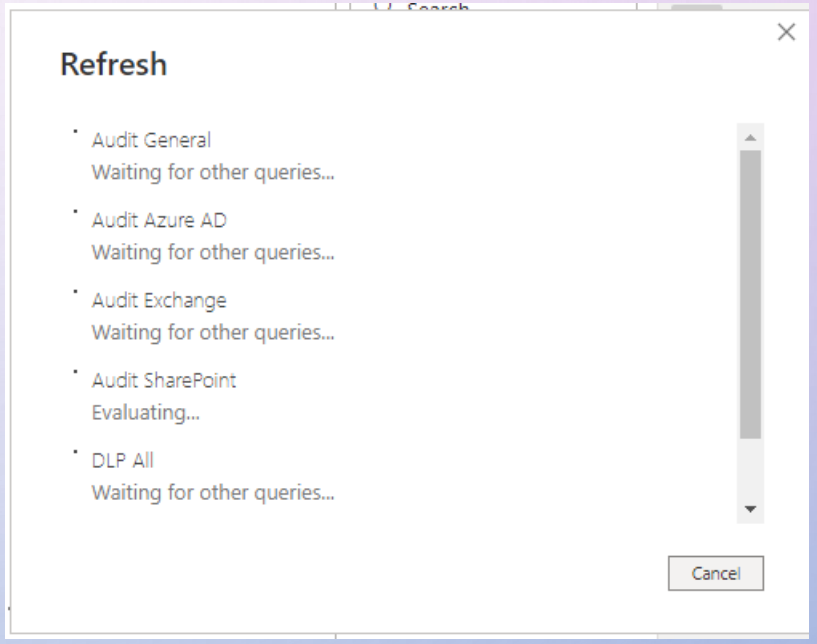


Microsoft

POWER BI

STEPS

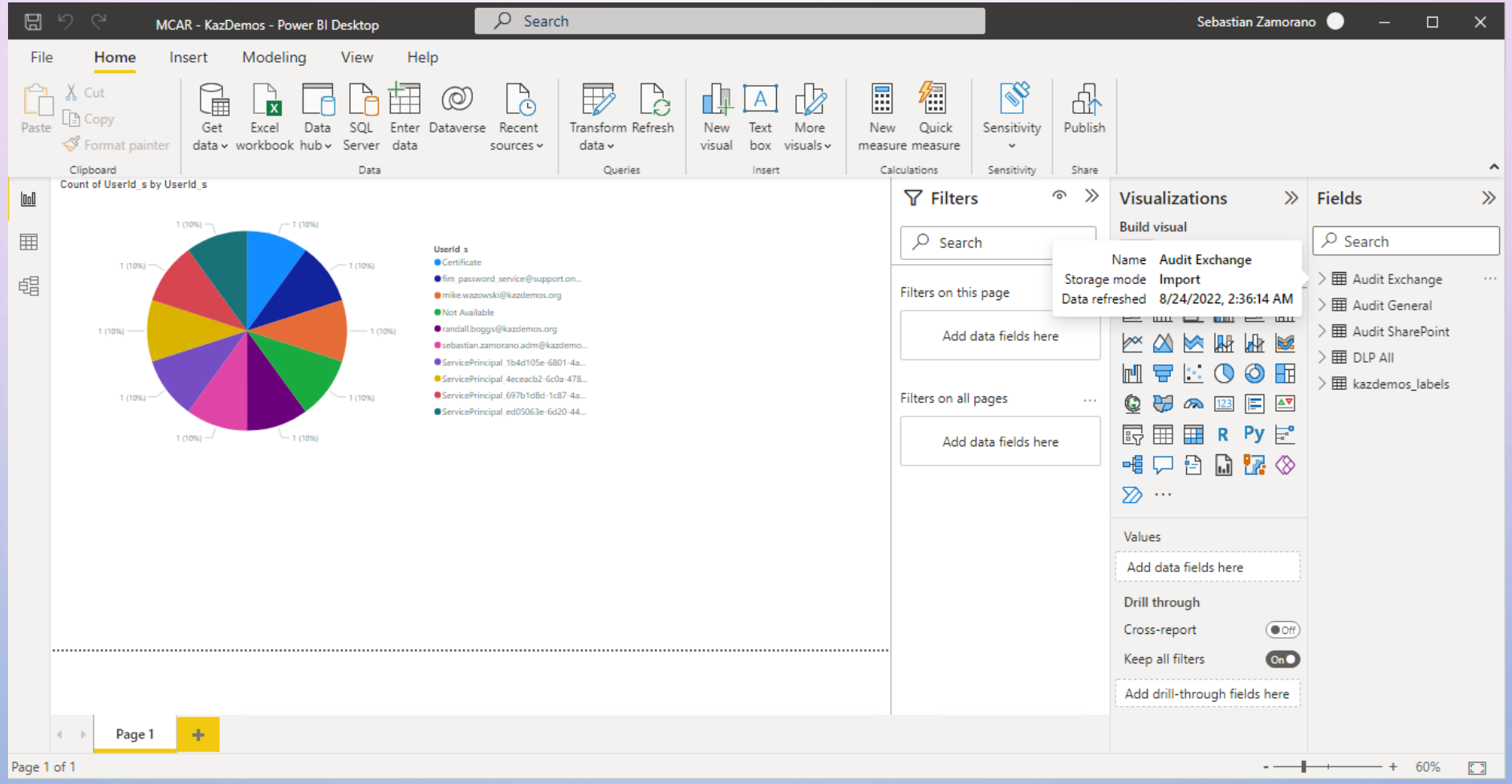




Microsoft

POWER BI

STEPS



POWER BI - TEMPLATES

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

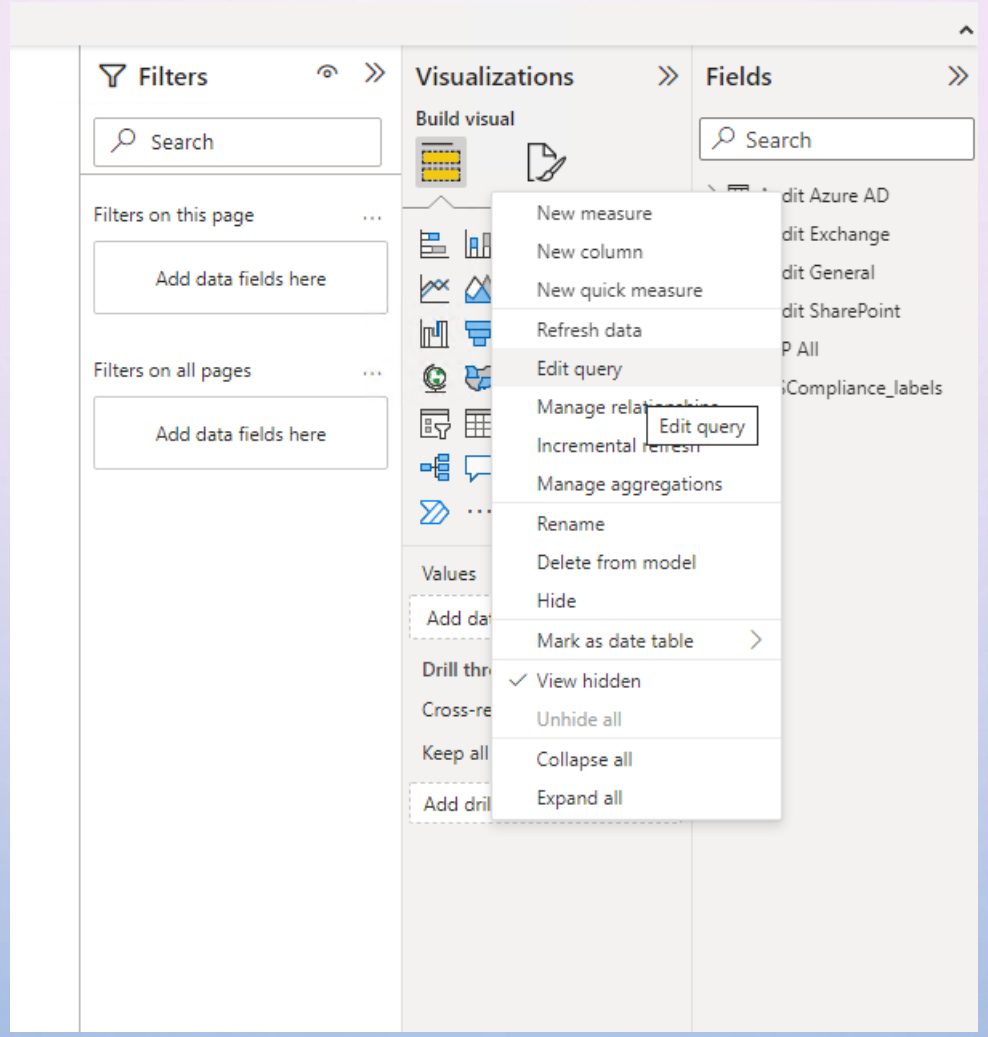
LET SOURCE = JSON.DOCUMENT(WEB.CONTENTS("HTTPS://API.LOGANALYTICS.IO/V1/WORKSPACES/"& WORKSPACE_ID &"/QUERY",

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

Microsoft

POWER BI - TEMPLATES

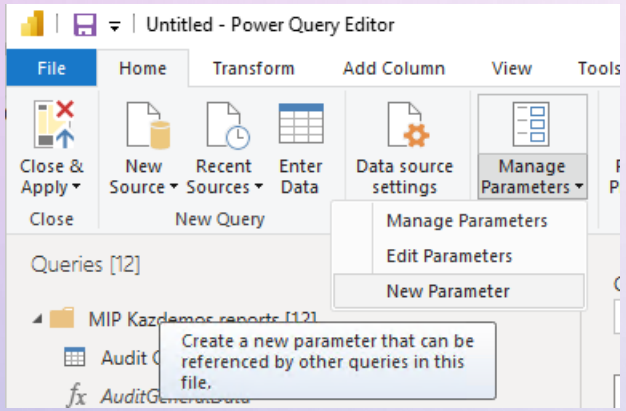
STEPS

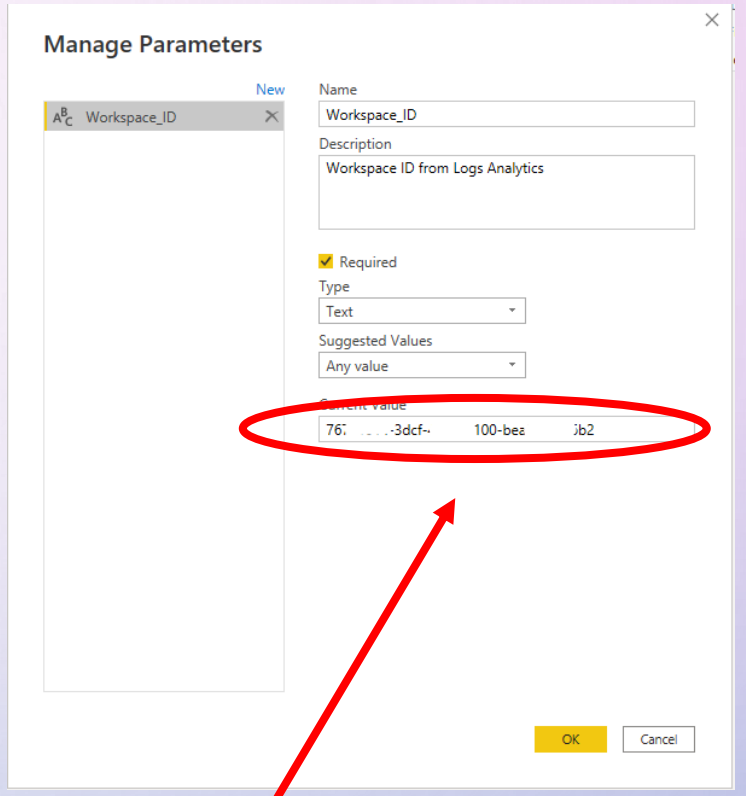


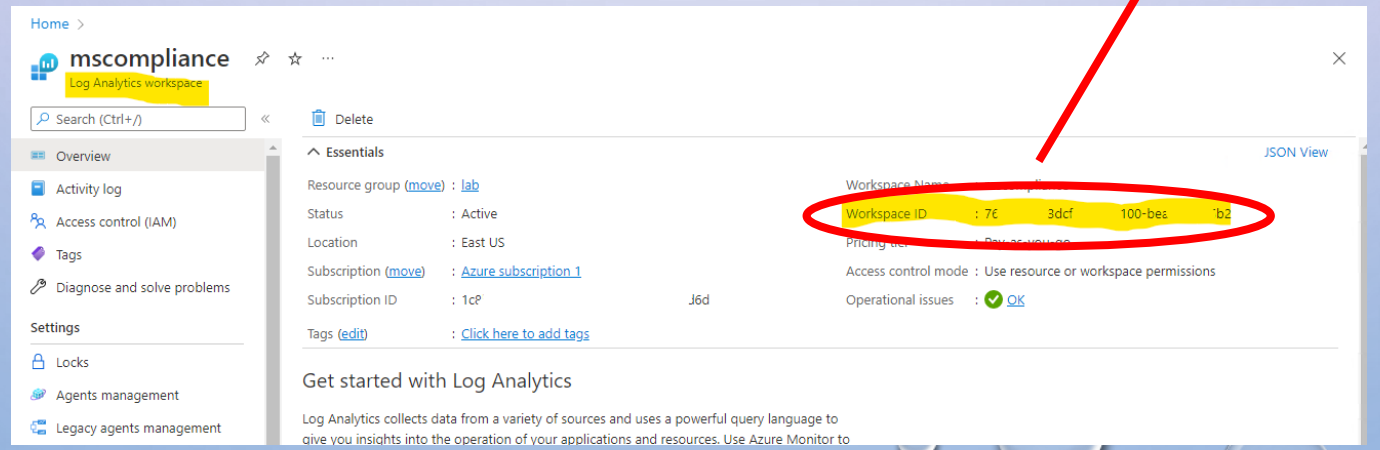
Microsoft

POWER BI - TEMPLATES

STEPS



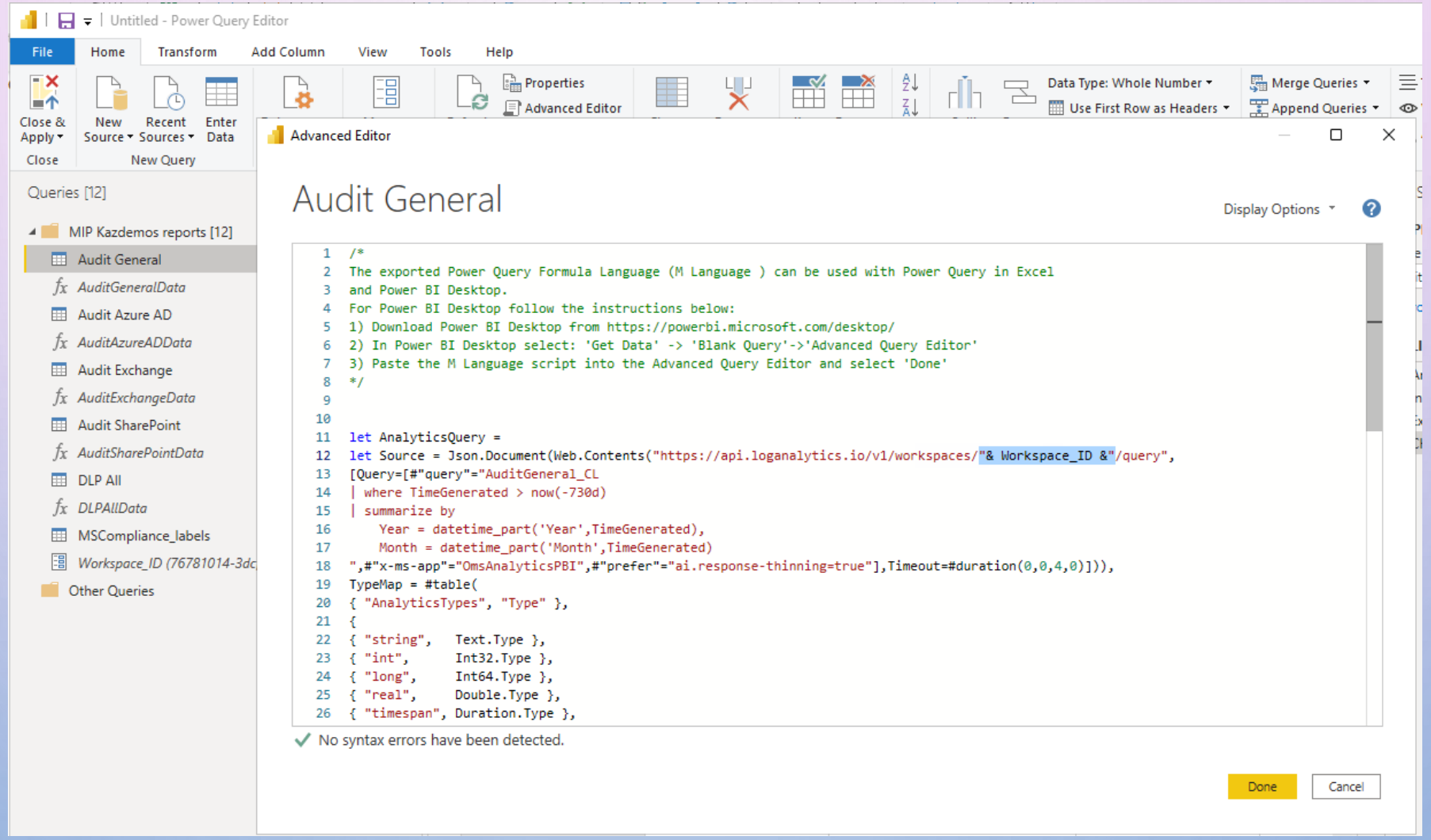




Microsoft

POWER BI - TEMPLATES

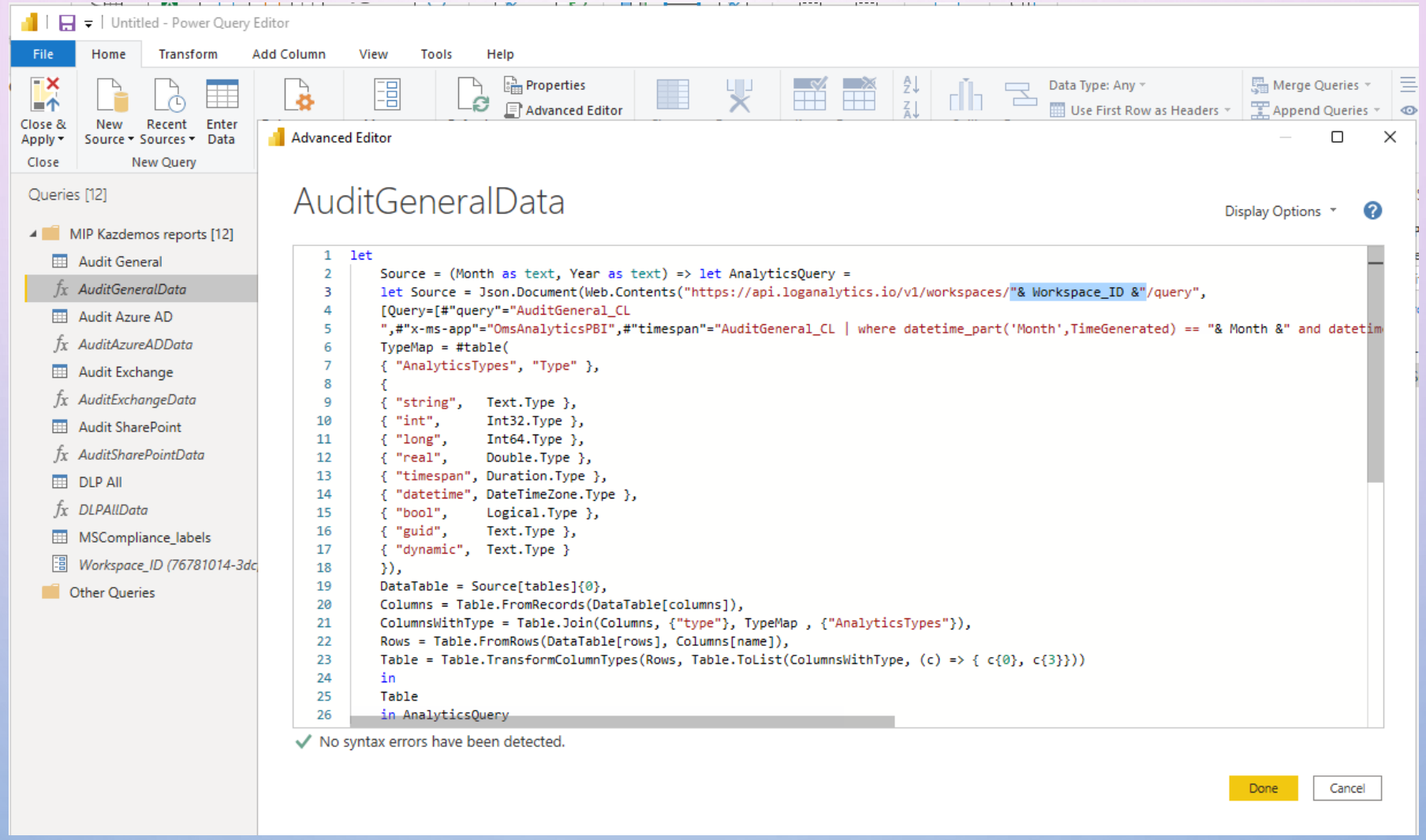
STEPS



Microsoft

POWER BI - TEMPLATES

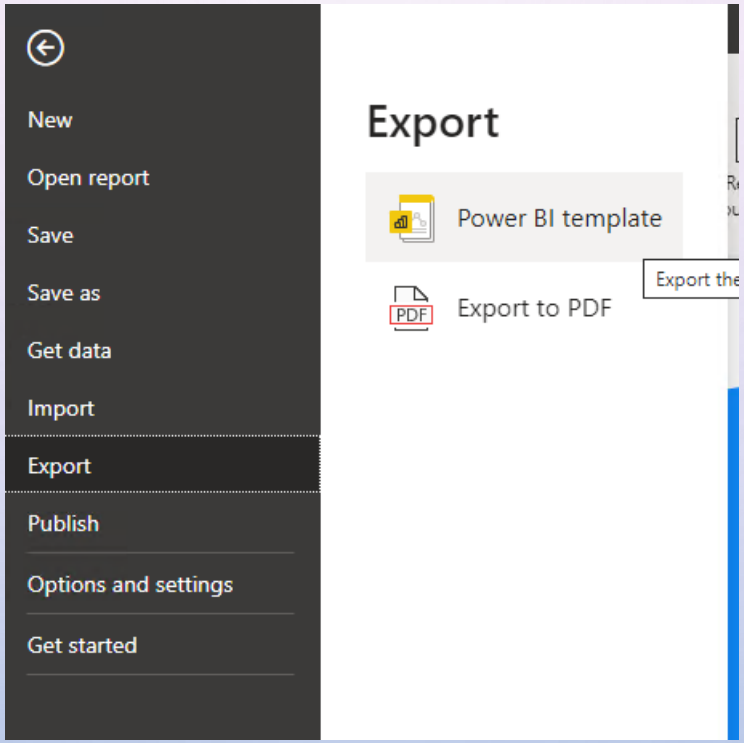
STEPS



Microsoft

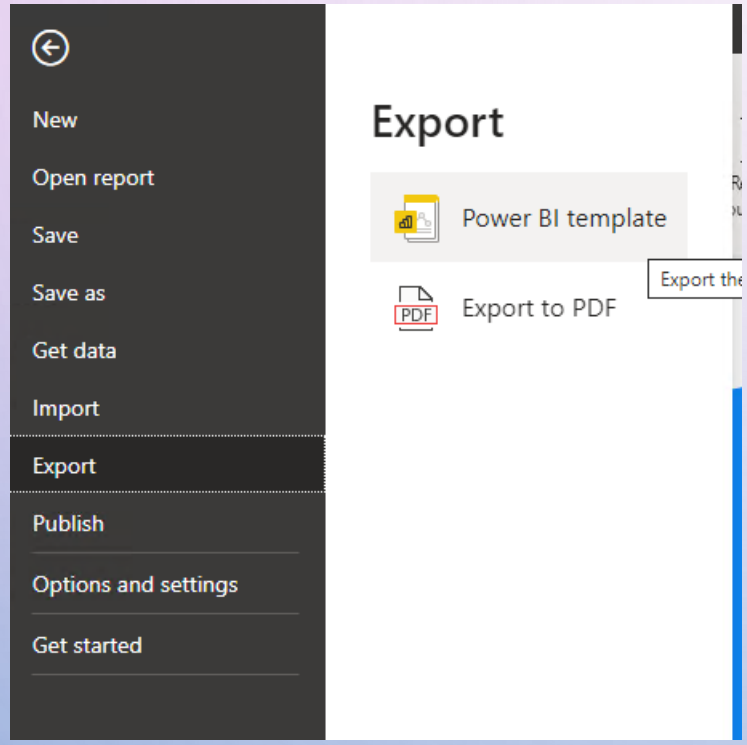
POWER BI - TEMPLATES

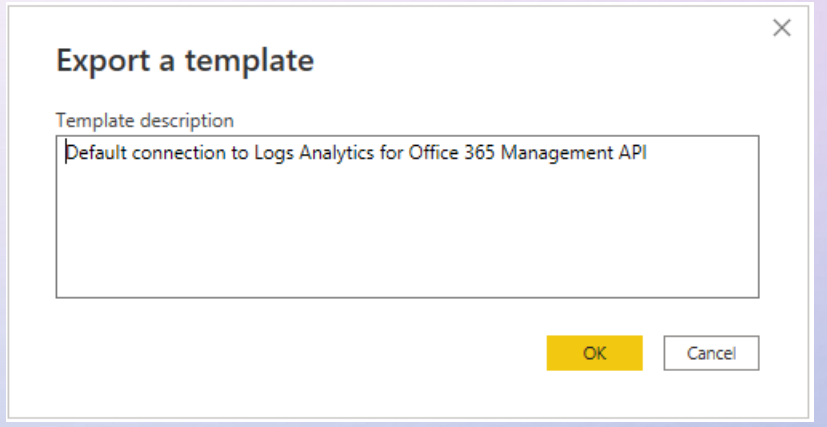
STEPS



POWER BI - TEMPLATES

STEPS

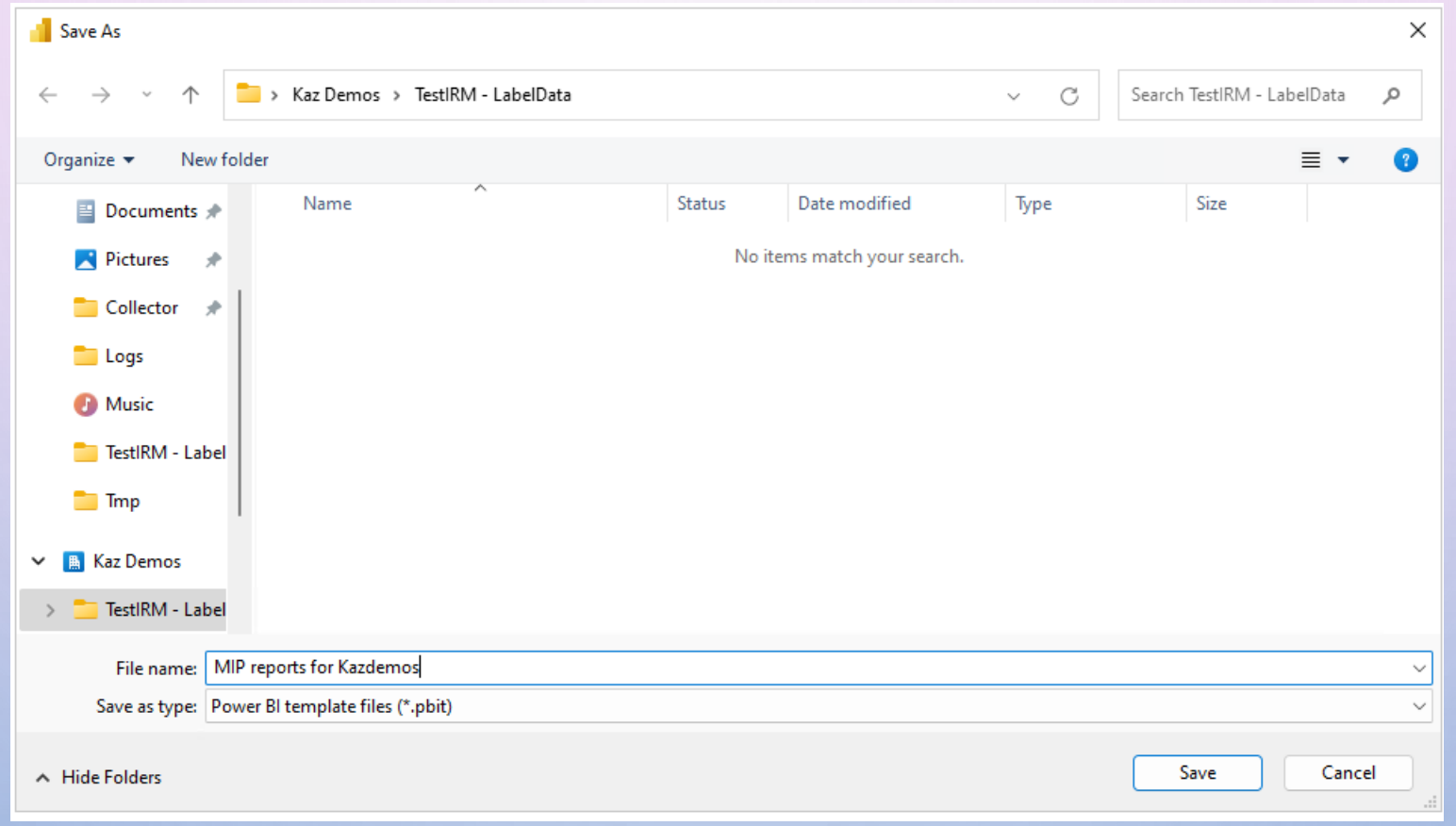




Microsoft

POWER BI - TEMPLATES

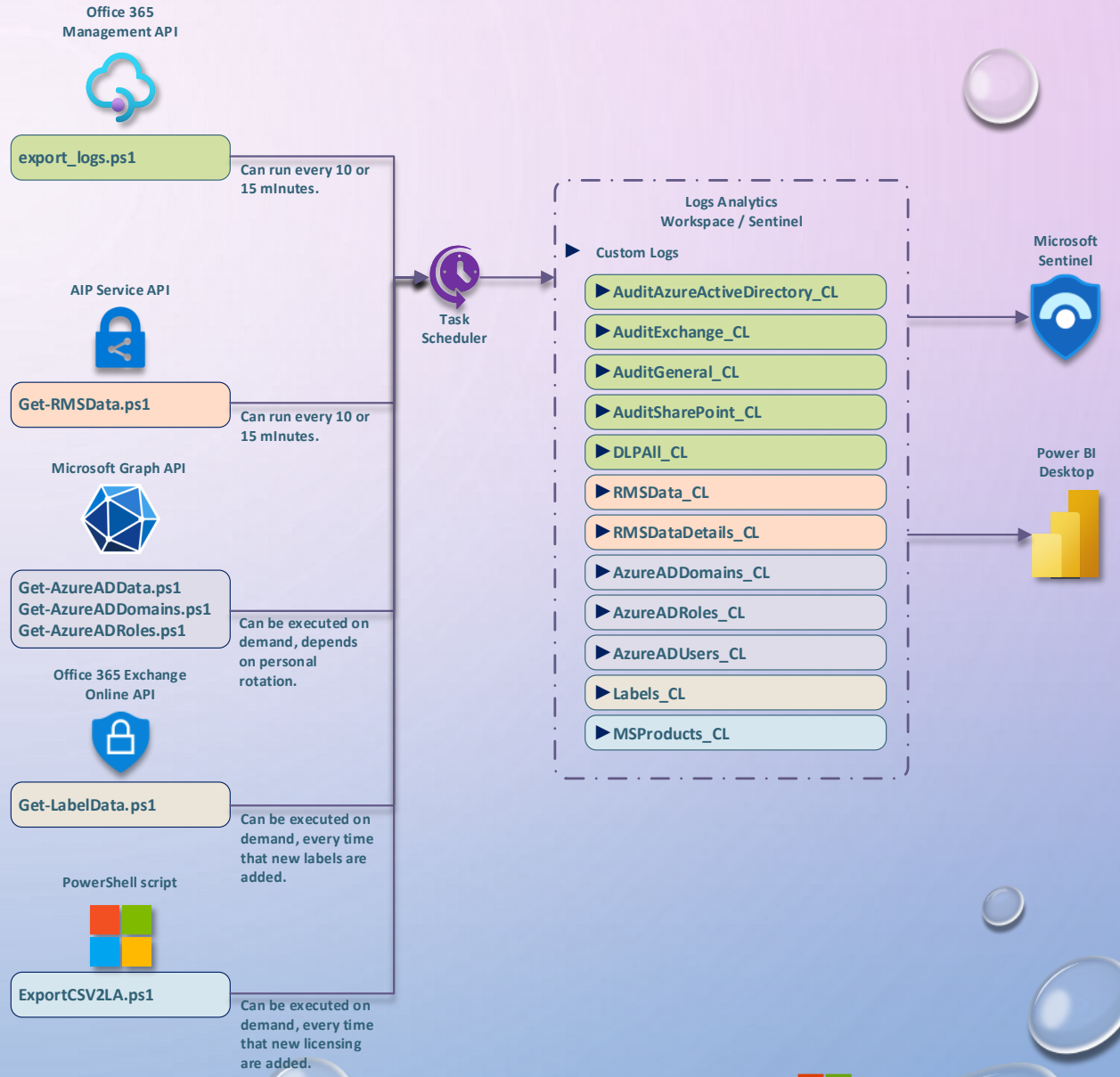
STEPS



CHECKLIST TO IMPORT POWER BI TEMPLATE

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

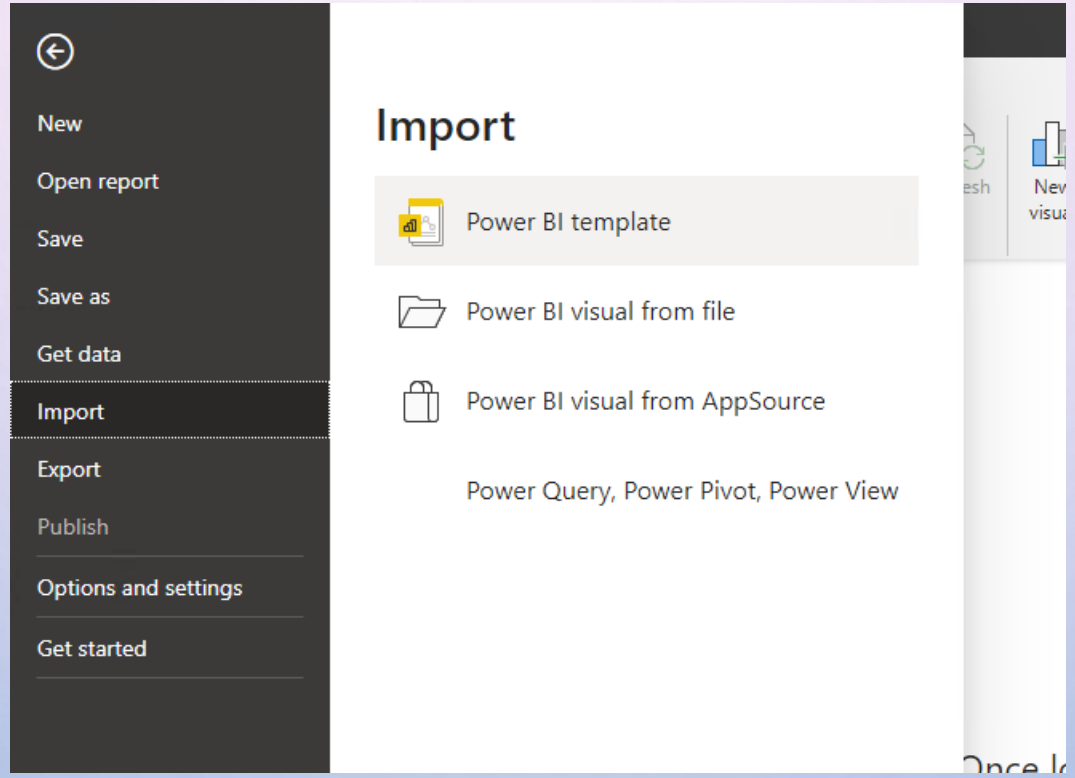


TO IMPORT A TEMPLATE

- 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

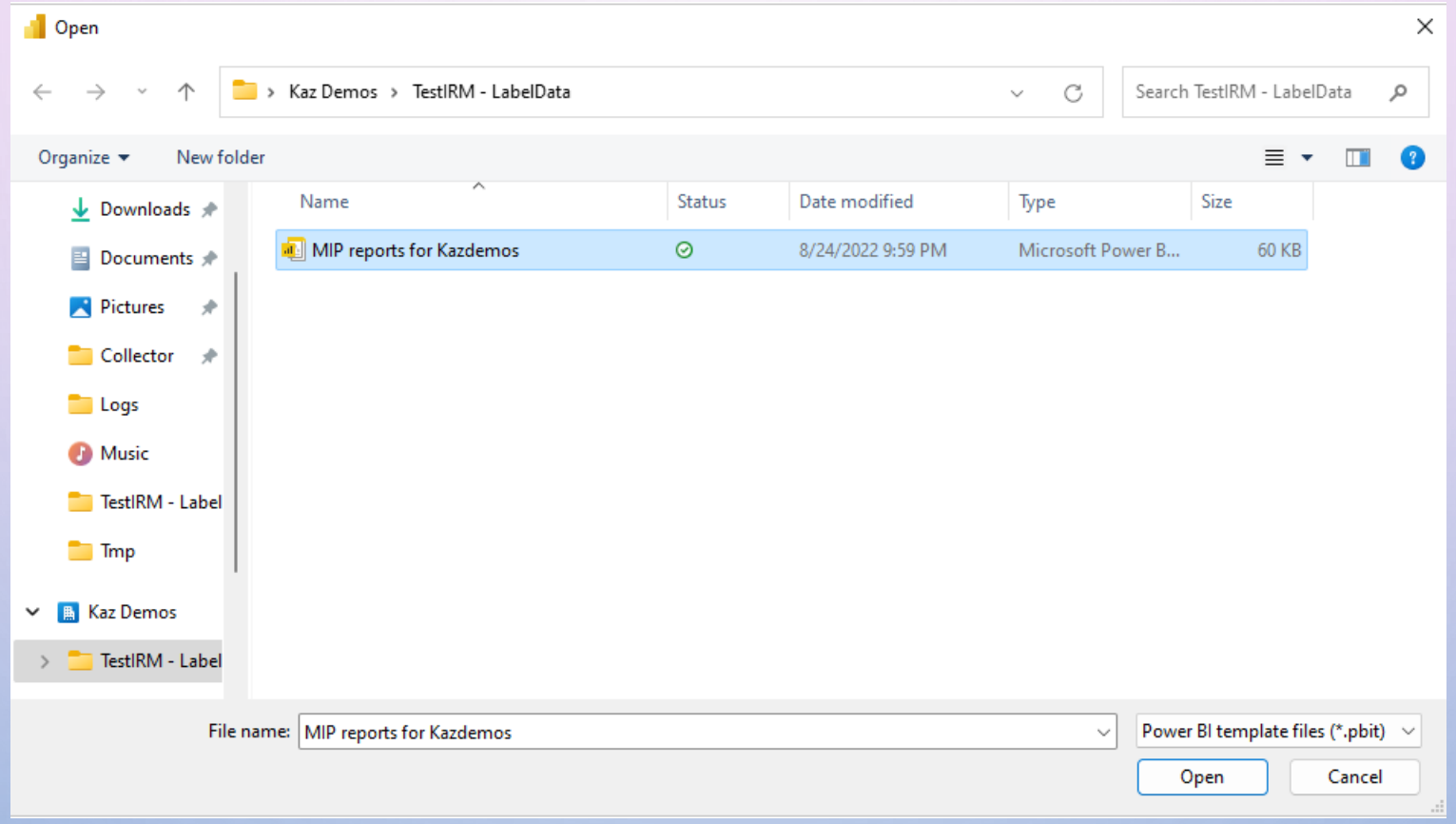
POWER BI - TEMPLATES

STEPS



POWER BI - TEMPLATES

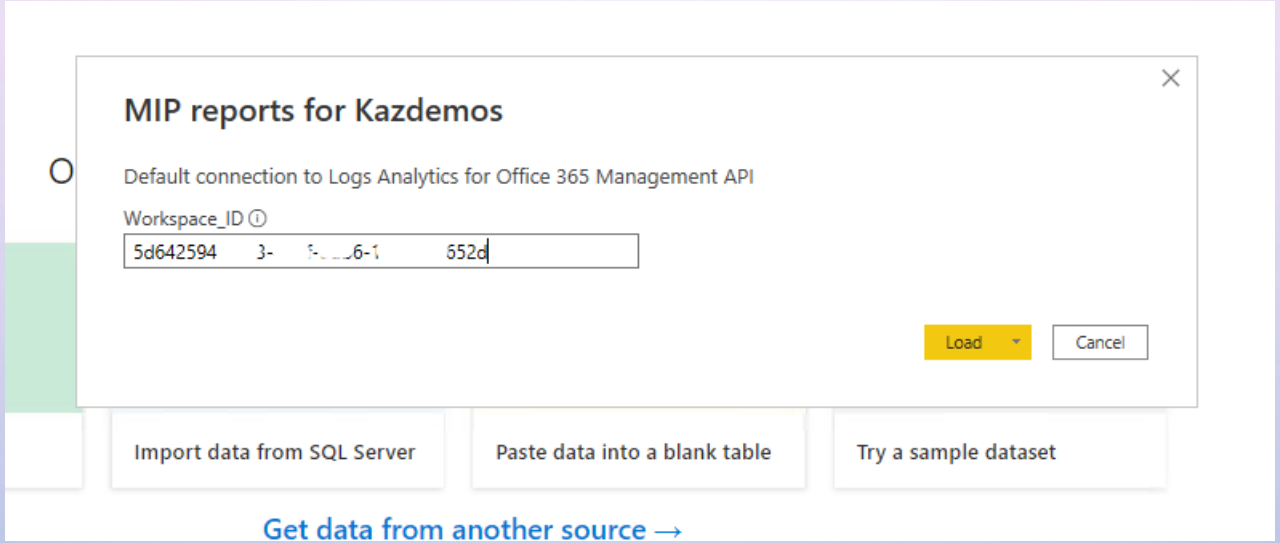
STEPS



Microsoft

POWER BI - TEMPLATES

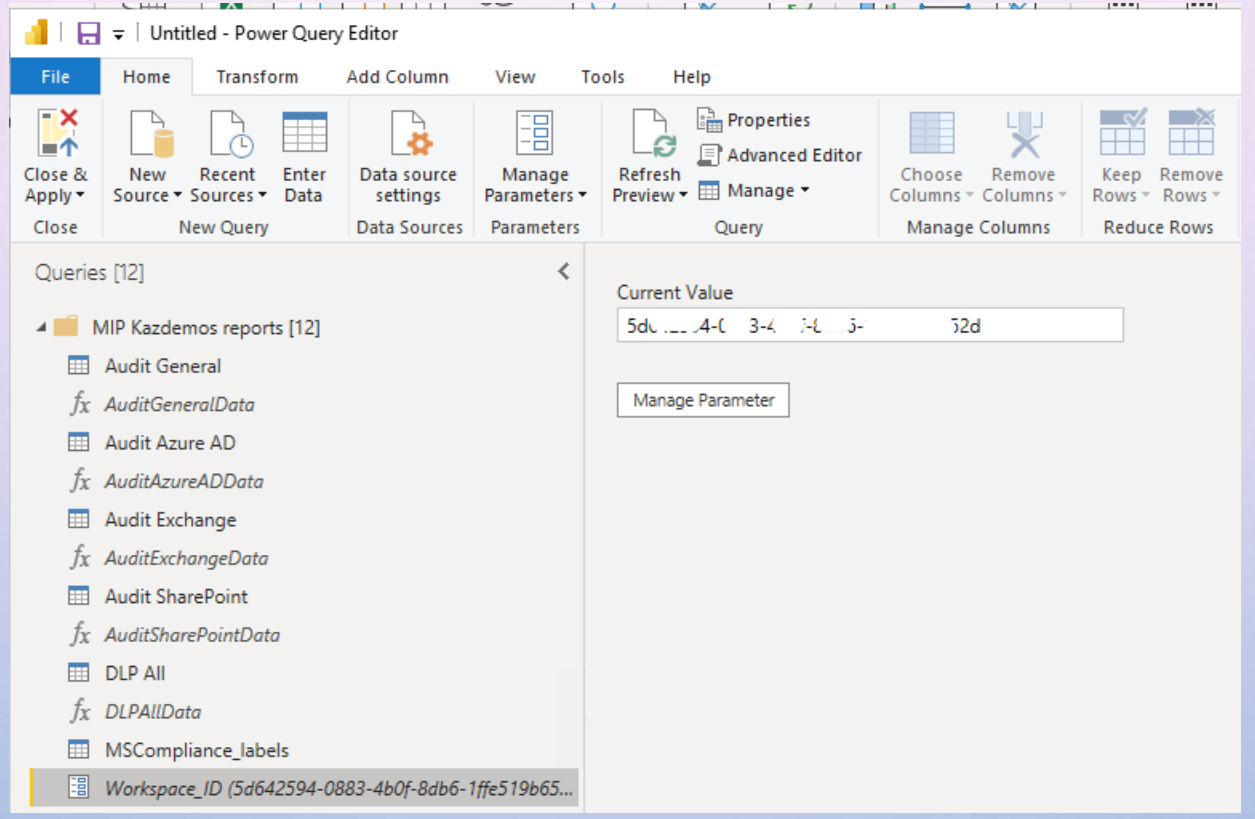
STEPS



Microsoft

POWER BI - TEMPLATES

STEPS



Microsoft

GEO LOCATION ON POWER BI

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"

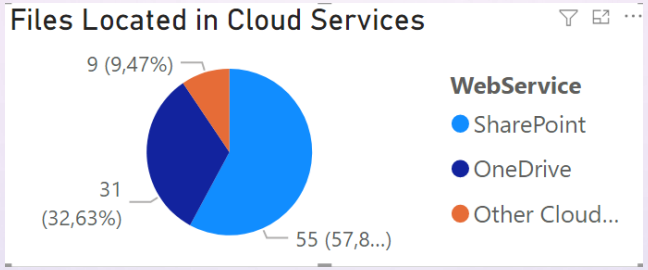
**This report uses an external service, https://ipwhois.io/, and can have additional costs*

Microsoft

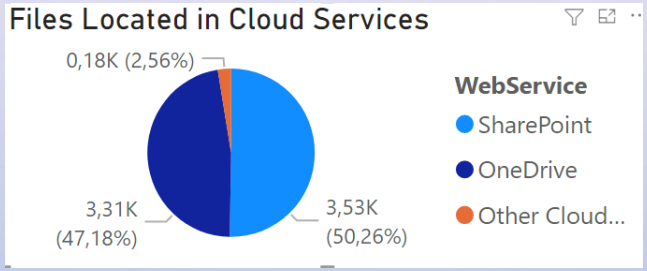
Tips

AVOID SOME BAD REPORTS

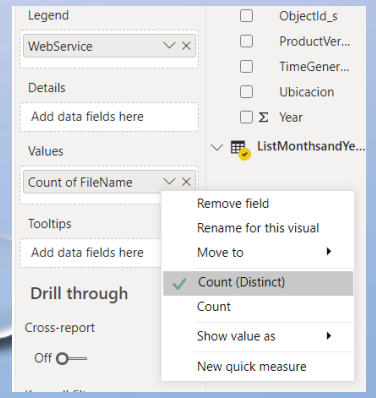
- SOMETIMES WE NEED TAKE CARE WITH THE VALUES AND FILTERS USED WHEN WE CREATE OUR REPORTS TO SHOW WRONG INFORMATION, HERE AN EXAMPLE:



- 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



Microsoft

Links

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

Microsoft

https://aka.ms/bingthrivekudos

THANK YOU

SEBASTIÁN ZAMORANO

+56 9 5207 3058

SEBASTIAN.ZAMORANO@MICROSOFT.COM

WWW.MICROSOFT.COM

myprofile.kazblog.me

Microsoft

TOPICS PENDING TO RELEASE

SOME ADDITIONAL EFFORT TO RELEASE SOON

- 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
- INCREMENTAL REFRESH ON POWER BI TO REDUCE LOGS ANALYTICS COST
- PUBLISH DIFFERENT REPORTS FOR SEPARATE AUDIENCE ON POWER BI ONLINE
- FIELDS DICTIONARY
- RELATIONSHIP MAP BETWEEN TABLES

Microsoft