Microsoft

Microsoft Purview Advanced Rich Reports **MPARR**

Installation Guide

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

(SEPTEMBER 2023)

Sebastián Zamorano A.
ISD Senior Consultant

https://aka.ms/MPARR-LinkedIn

https://aka.ms/MPARR-GitHub

https://aka.ms/MPARR-Youtube

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.

And several other people that is believe on me and this crazy idea.

Really thanks to all

Sebastián Andrés Zamorano Andrade

AGENDA

WHAT WILL WE HAVE FOUND HERE?

Agenda

What will we have found here?

- Samples of reports that can be created
- General concepts
- Requirements
- Baseline configuration
- KQL samples
- Power BI connection
- Advanced Settings and tips

Microsoft

DASHBOARDS

SOME SAMPLE REPORTS

Dashboard for Unified Labeling behavior

Dashboard - Overview

Unified Labeling
Overview

3,822
Number of files

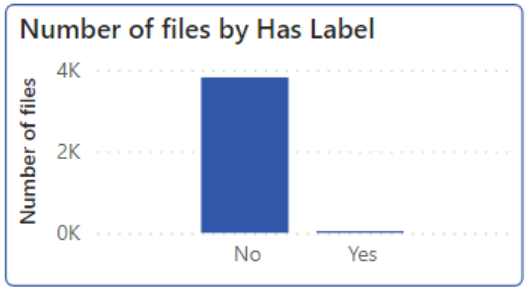
759
Number of user owned files

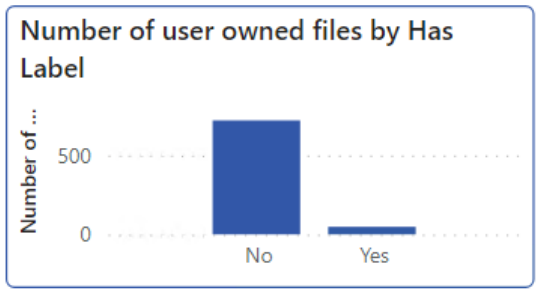
48
Number of labeled files

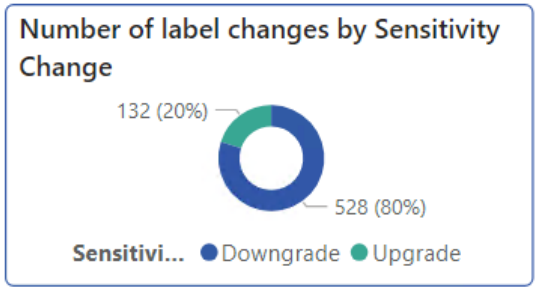
Filtering

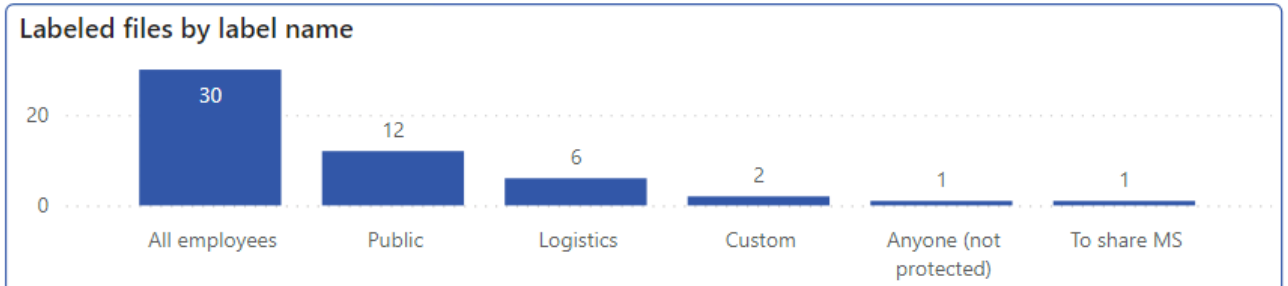
Department: HR

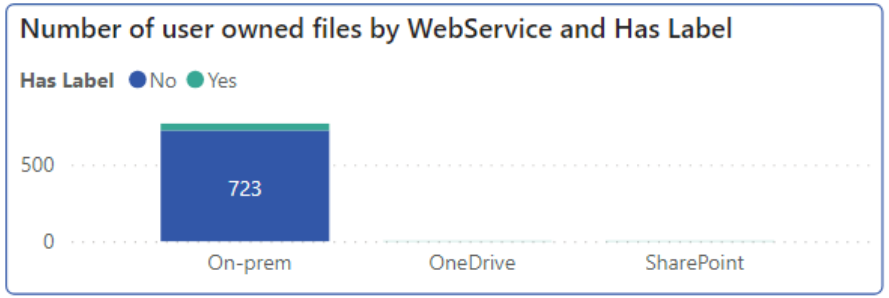
Country_s: All

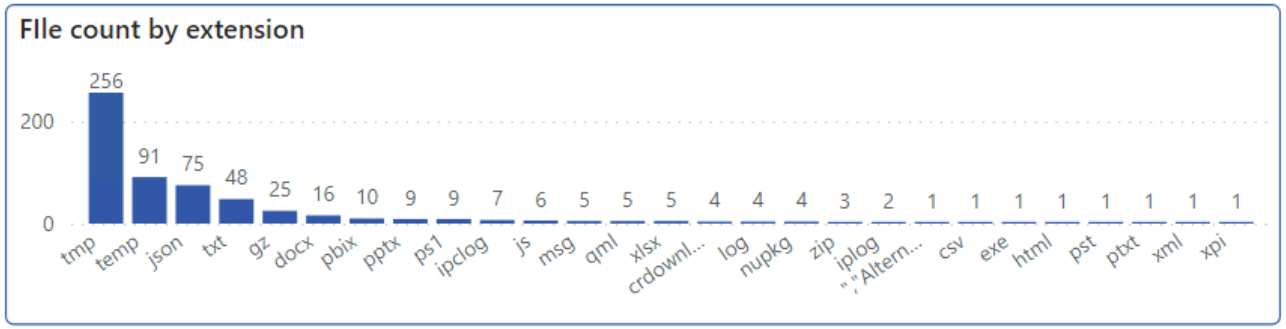








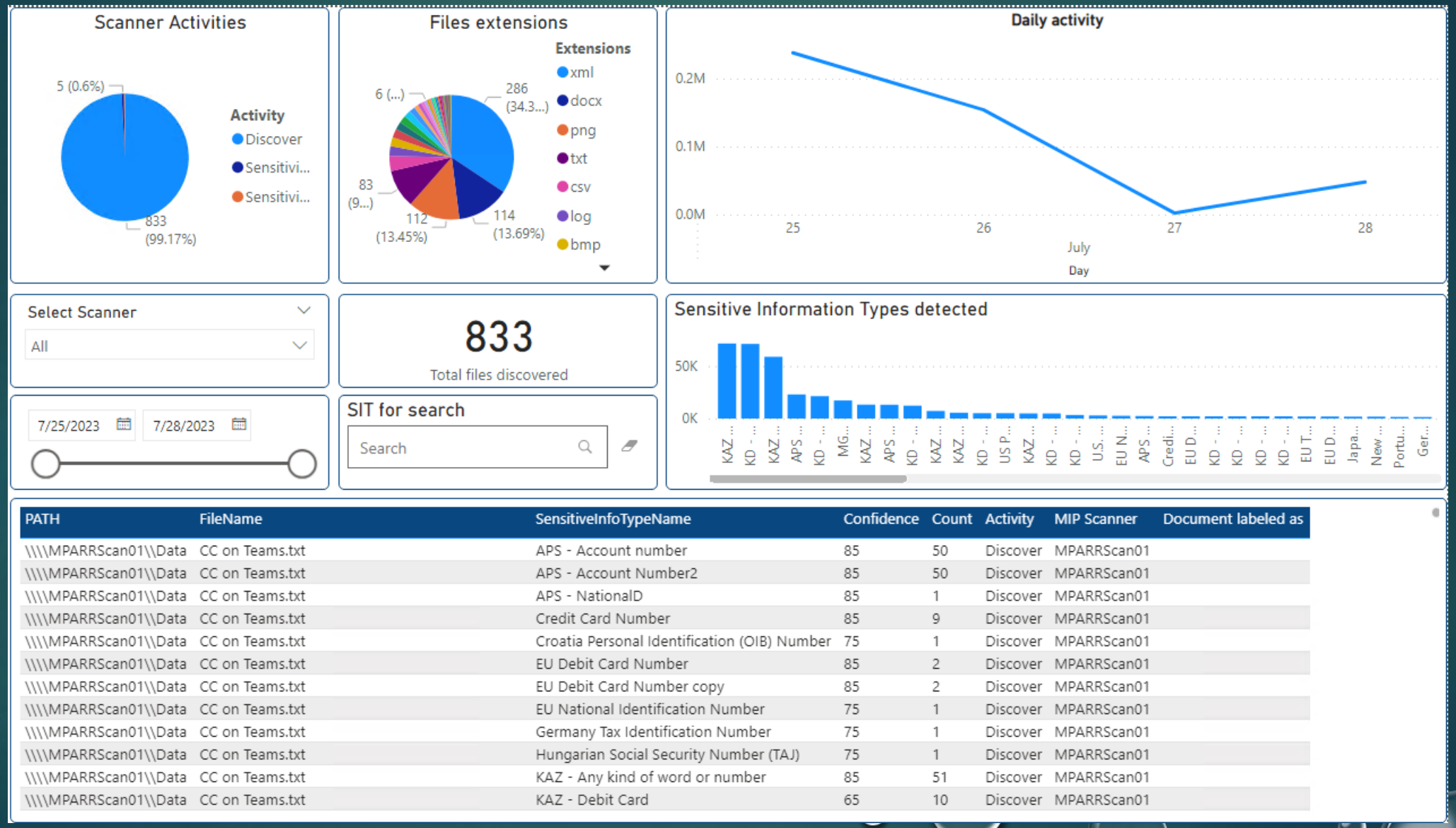




User
dominik.kot@kazdemos.org
randall.boggs@kazdemos.org

Dashboard – MIP Scanner

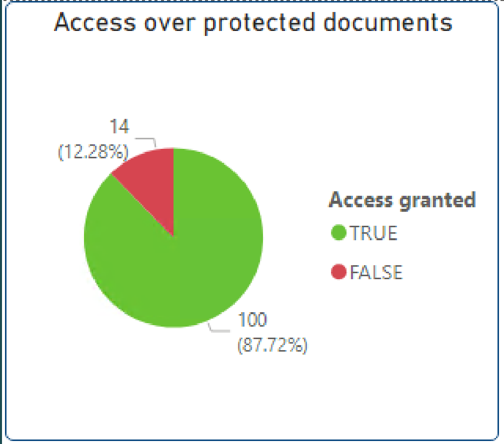
Dashboard for MIP Scanner activities

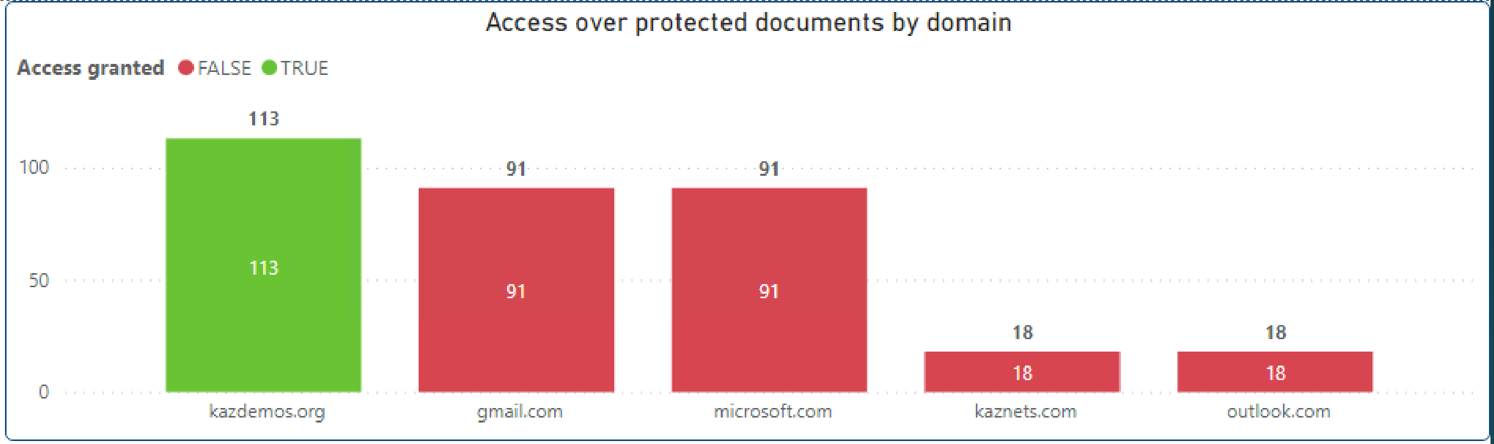


PATH	FileName	SensitiveInfoTypeName	Confidence	Count	Activity	MIP Scanner	Document labeled as
\\\\MPARRScan01\\Data	CC on Teams.txt	APS - Account number	85	50	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	APS - Account Number2	85	50	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	APS - NationalD	85	1	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	Credit Card Number	85	9	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	Croatia Personal Identification (OIB) Number	75	1	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	EU Debit Card Number	85	2	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	EU Debit Card Number copy	85	2	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	EU National Identification Number	75	1	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	Germany Tax Identification Number	75	1	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	Hungarian Social Security Number (TAJ)	75	1	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	KAZ - Any kind of word or number	85	51	Discover	MPARRScan01	
\\\\MPARRScan01\\Data	CC on Teams.txt	KAZ - Debit Card	65	10	Discover	MPARRScan01	

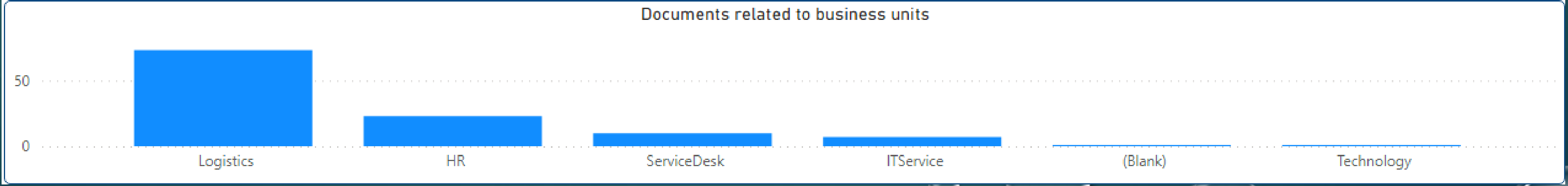
Dashboard – RMS Protection

Dashboard for access granted and denied for protected documents



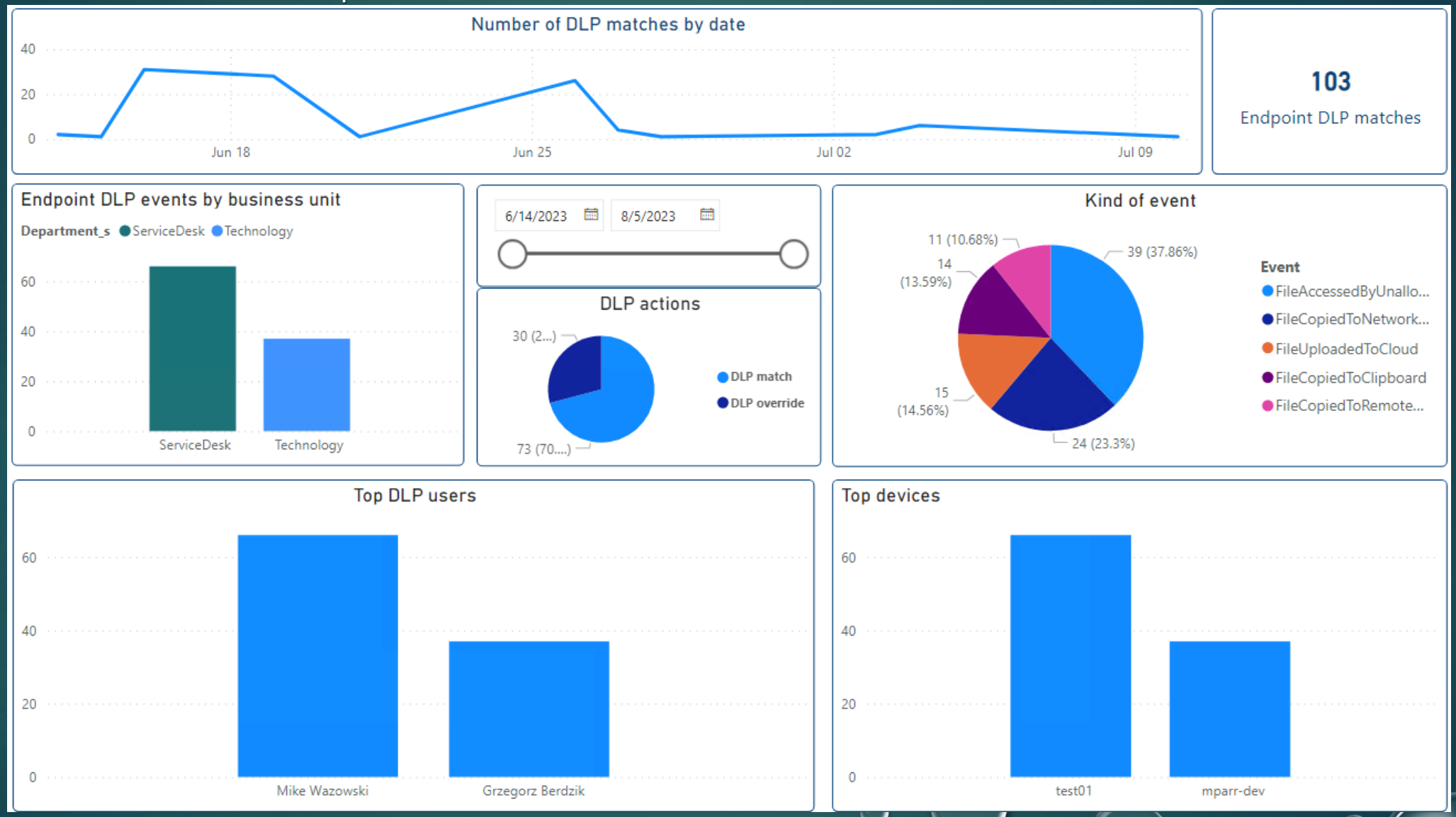


External email	Permissions granted	Who protecte
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD,OBJMODEL"]	mike.wazowski@kazd
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD,OBJMODEL"]	mike.wazowski@kazd
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	randall.boggs@kazde
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	randall.boggs@kazde
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	randall.boggs@kazde
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	randall.boggs@kazde
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,EDITRIGHTSDATA,EXPORT,OBJMODEL,OWNER"]	sebastian.zamorano.a
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD,OBJMODEL"]	mike.wazowski@kazd
grzegorz.berdzik@kazdemos.org	["VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,REPLY,REPLYALL,FORWARD,OBJMODEL"]	mipscanner@kazdem



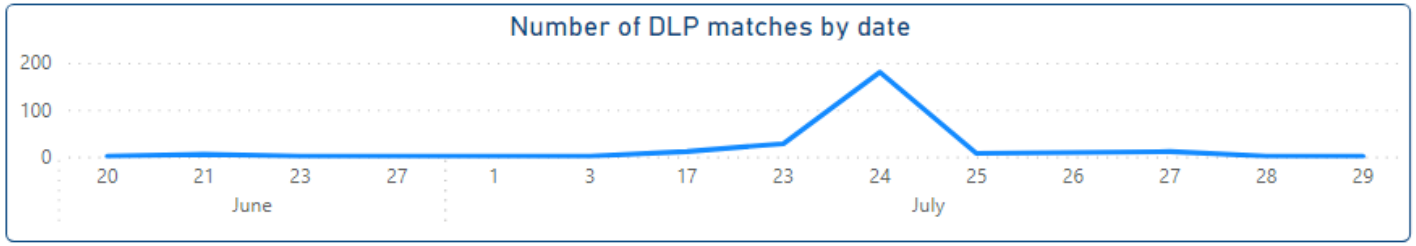
Dashboard – Endpoint DLP

Dashboard for endpoint DLP activities



Dashboard for SPO DLP detailed activities

Dashboard – DLP Details



252

Rules matches

M365 Service: All

SIT name: credit

User: Search

File name: Search

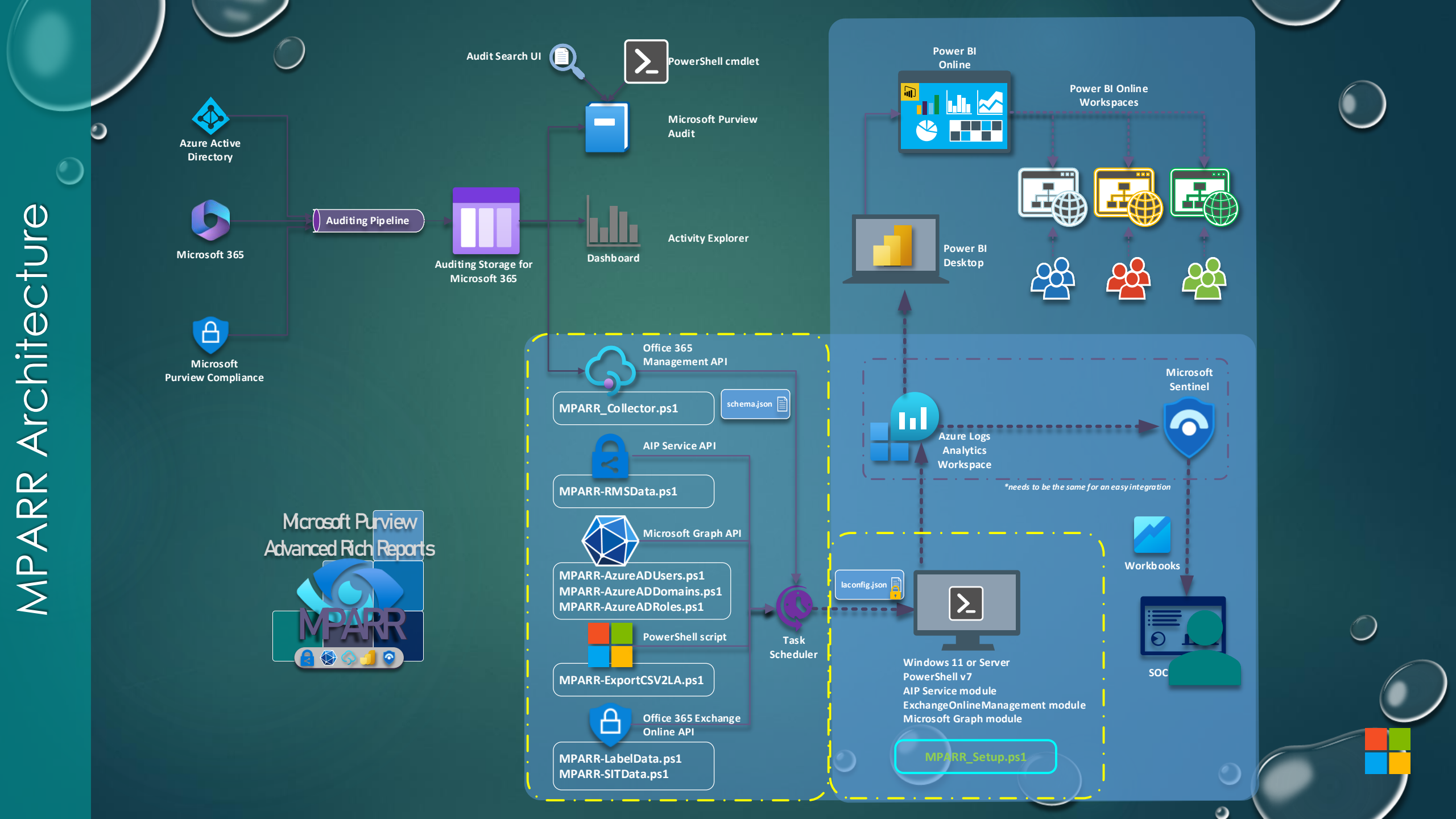
6/20/2023 7/29/2023

M365 Service	File name	File size	File owner	URL Path	SITs	Count
SharePoint	Error_DLP.All_05-28-2023_04-47-39.json	39376	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Error_DLP.All_05-28-2023_11-02-39.json	6979	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Error_DLP.All_05-28-2023_11-47-39.json	773602	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Error_DLP.All_05-29-2023_05-47-39.json	758893	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Error_DLP.All_05-29-2023_09-32-39.json	1896205	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Error_DLP.All_05-30-2023_01-32-39.json	1516984	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	New test files 5-15-2023.zip	230225	Grzegorz Berdzik	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	numbers.txt	898	Grzegorz Berdzik	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	numbers.txt	898	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Webinar.zip	218961	Grzegorz Berdzik	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	Webinar.zip	218961	Mike Wazowski	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	14
SharePoint	EmployeeDatabase.xlsx	32342	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/ExternalAccess	Credit Card Number	16
SharePoint	EmployeeDatabase.xlsx	26679	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	16
SharePoint	EmployeeDatabase.xlsx	26938	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	16
SharePoint	EmployeeDatabase.xlsx	31851	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	16
SharePoint	EmployeeDatabase.xlsx	33867	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	16
SharePoint	EmployeeDatabase - with errors.csv	8823	Mike Wazowski	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	2
SharePoint	EmployeeDatabase - without SSN.csv	8219	Mike Wazowski	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	2
OneDrive	EmployeeDatabase-witherrors.csv	8823	Mike Wazowski	https://m365x089236-my.sharepoint.com/personal/mike_wazowski_kazdemos_org	Credit Card Number	2
SharePoint	Error_DLP.All_05-25-2023_04-32-39.json	99500	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	2
OneDrive	my ccs.docx	19899	Sebastian Zamorano (MCS)	https://m365x089236-my.sharepoint.com/personal/sebastian_zamorano_adm_kazdemos_org	Credit Card Number	2
OneDrive	my ccs-MCAR01.docx	19362	Sebastian Zamorano (MCS)	https://m365x089236-my.sharepoint.com/personal/sebastian_zamorano_adm_kazdemos_org	Credit Card Number	2
OneDrive	CC info.txt	2004	Sebastian Zamorano (MCS)	https://m365x089236-my.sharepoint.com/personal/sebastian_zamorano_adm_kazdemos_org	Credit Card Number	20
SharePoint	FOLDER1_DDT_POC_Word_PIIs.docx	43425	Darren Bonehill	https://m365x089236.sharepoint.com/sites/DWB-Test	Credit Card Number	20
SharePoint	Datos de prueba - copia.xlsx	53351	Sebastian Zamorano (MCS)	https://m365x089236.sharepoint.com/sites/MPARR	Credit Card Number	213

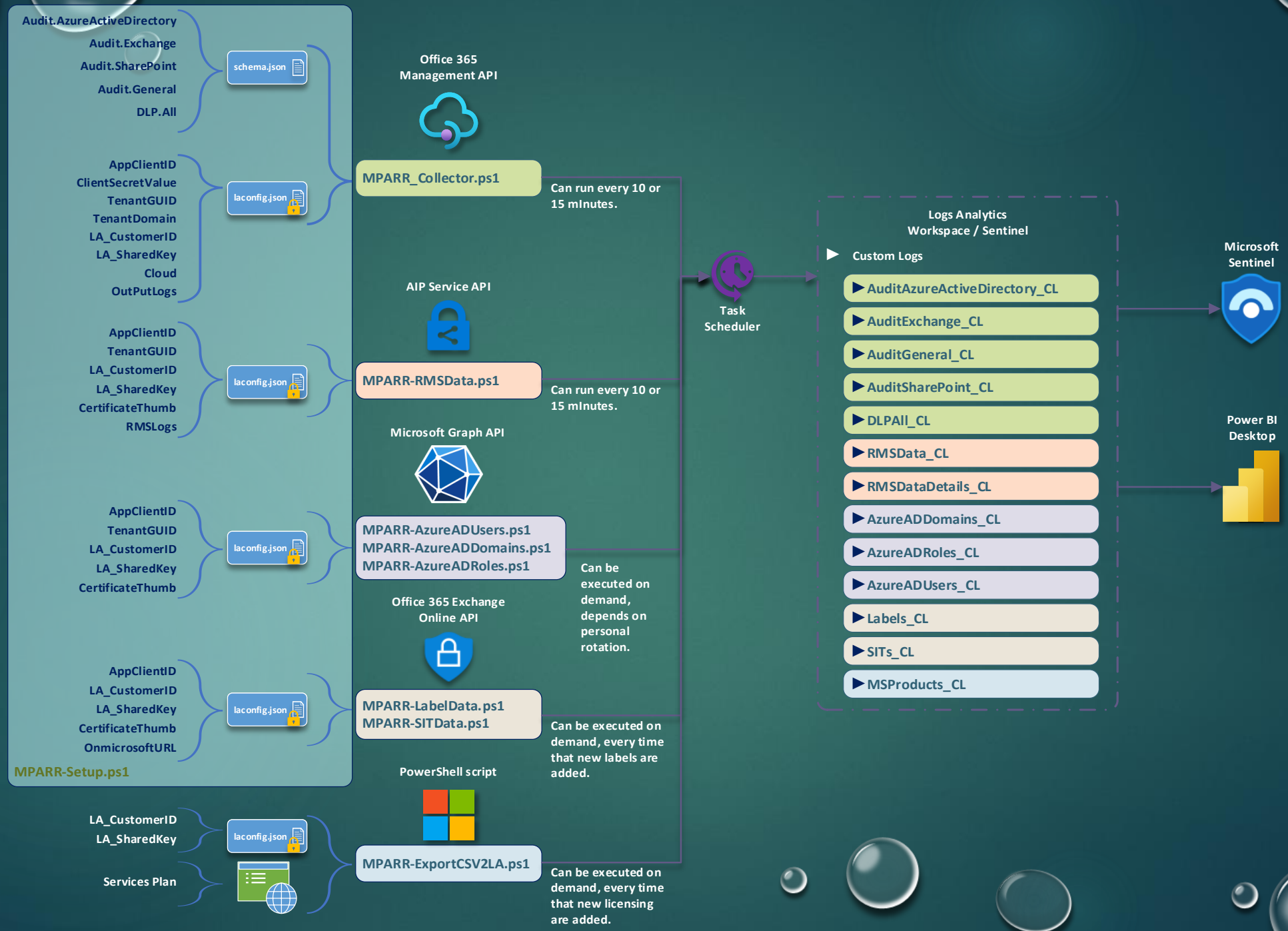
SOME STUFFS TO TAKE ON MIND

Capabilities to implement previously reports shown depends to implement MPARR as your solution to collect all the information available through Office 365 Management API, and supporting APIs, if some of the scripts are not implemented, the reports can be not implemented in the right way.

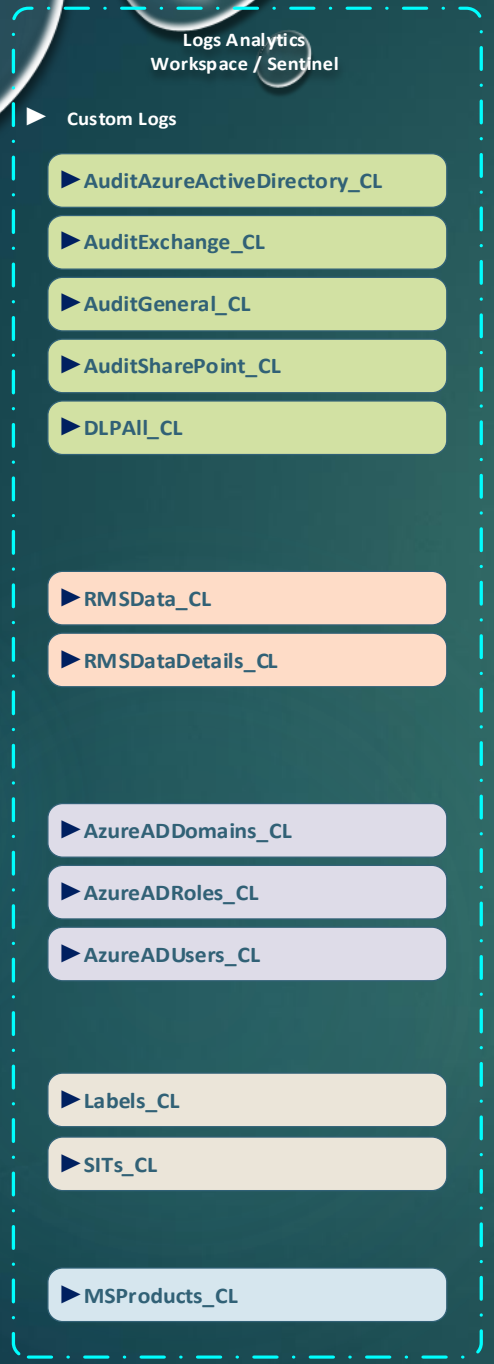
MPARR Architecture



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. Additionally, a table is created with the Sensitive Information Types using names and Ids.

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.

Brief description about MPARR installation

To deploy and configure MPARR we need to consider these steps:

- You need to install PowerShell 7 in the computer used for MPARR
- You need to create a workspace in Logs Analytics
- You need to download MPARR from https://aka.ms/MPARR-GitHub
- You need to execute MPARR_Setup.ps1
- You need grant permissions to the APIs used by the Azure AD App created on the previous step
- Add permissions on the task in task scheduler to run as a service

In the next slides you will see all the steps in details.

Requirements

Requirements to implement MPARR

- Logs Analytics workspace (Azure subscription)
- Workstation with Windows 10/11 or Server with Windows Server 2016+ with Internet access
- PowerShell v7 installed on the previous machine
- MPARR_Setup.ps1 install these PowerShell latest modules:
  - AIPService
  - Az.Accounts
  - Az.OperationalInsights
  - Az.Resources
  - Microsoft.Graph.Applications
  - Microsoft.Graph.Users
  - Microsoft.Graph.Identity.DirectoryManagement
- MPARR_Setup.ps1 needs Global Administrator role to be executed
- An Azure subscription admin account to create the workspace under Logs Analytics service
- Compliance administrator role to obtain Sensitivity Labels list and Sensitive Information Types, this in the case to avoid use elevate privileges for MPARR_LabelData.ps1 and MPARR-SITData.ps1 scripts
- 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**
  - **https://aka.ms/MPARR-GitHub**
  - **https://github.com**

Microsoft

Index

GO DIRECTLY FROM HERE TO THE SPECIFIC TOPICS

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

By default, a workspace only retains data for 30 days, is recommended extend for at least 1 year to have historical data.

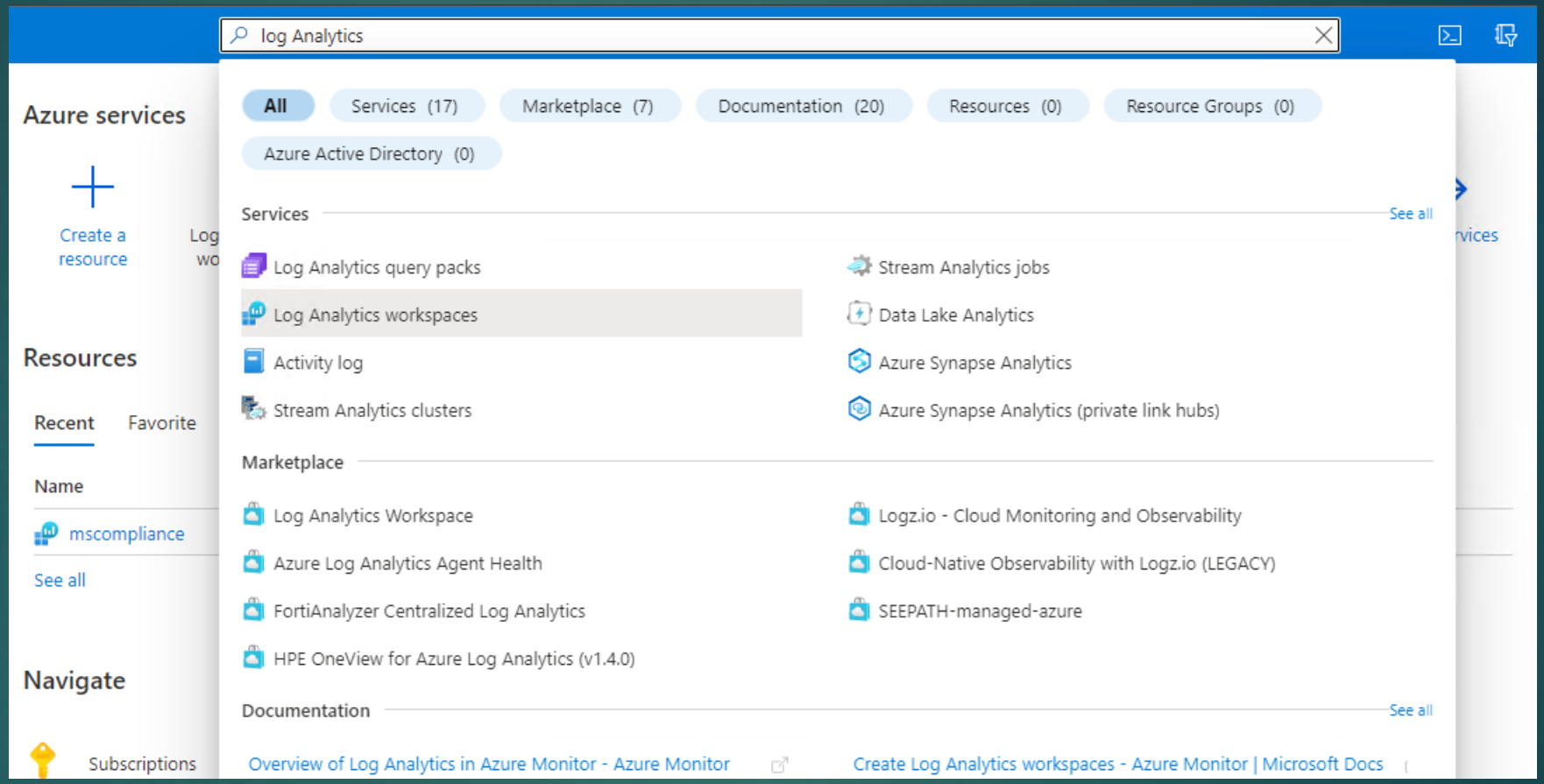
- Go to the Logs Analytics workspace, you can press "Go to resource" button after the previous steps are finished
- On the left pane select "Usage and estimated costs", and then at the top menu select "Data Retention" and extend to the time that you want to retain.

To **integrate with **Sentinel** the same Logs Analytics workspace is needed to be use.*

Microsoft

Logs Analytics workspace

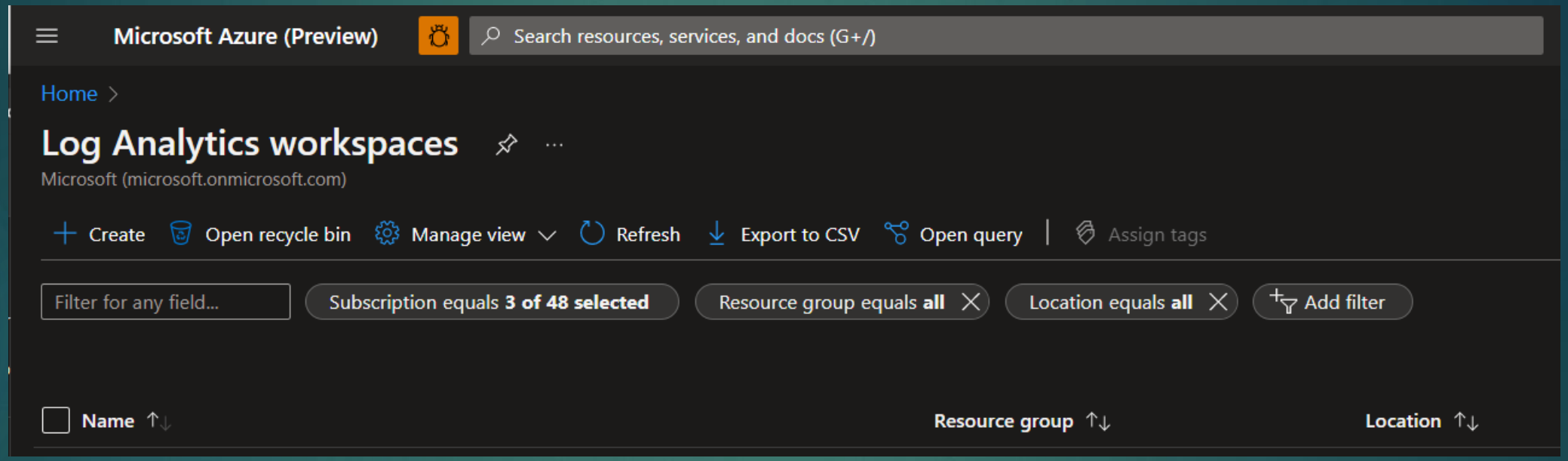
Steps



Microsoft

Logs Analytics workspace

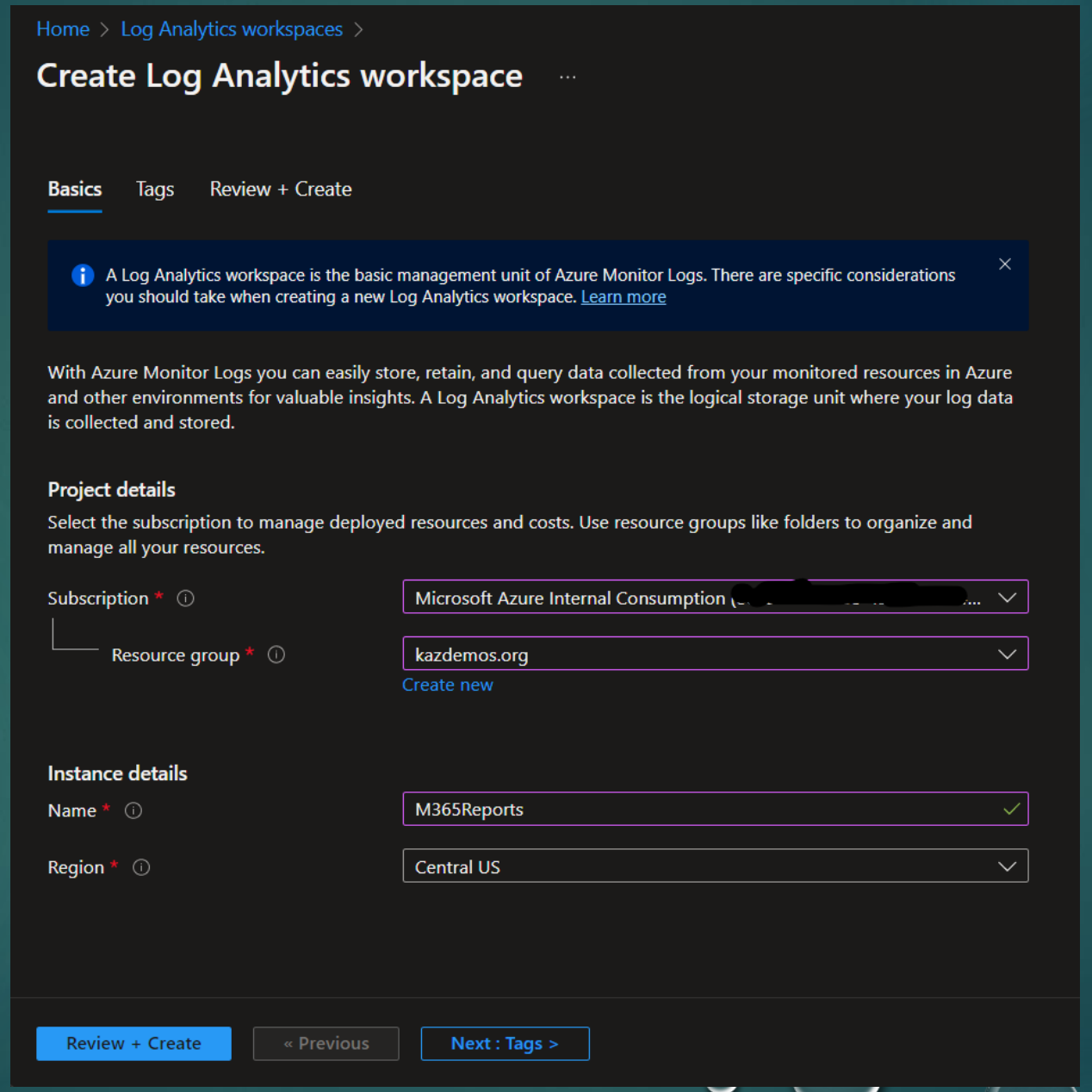
Steps



Microsoft

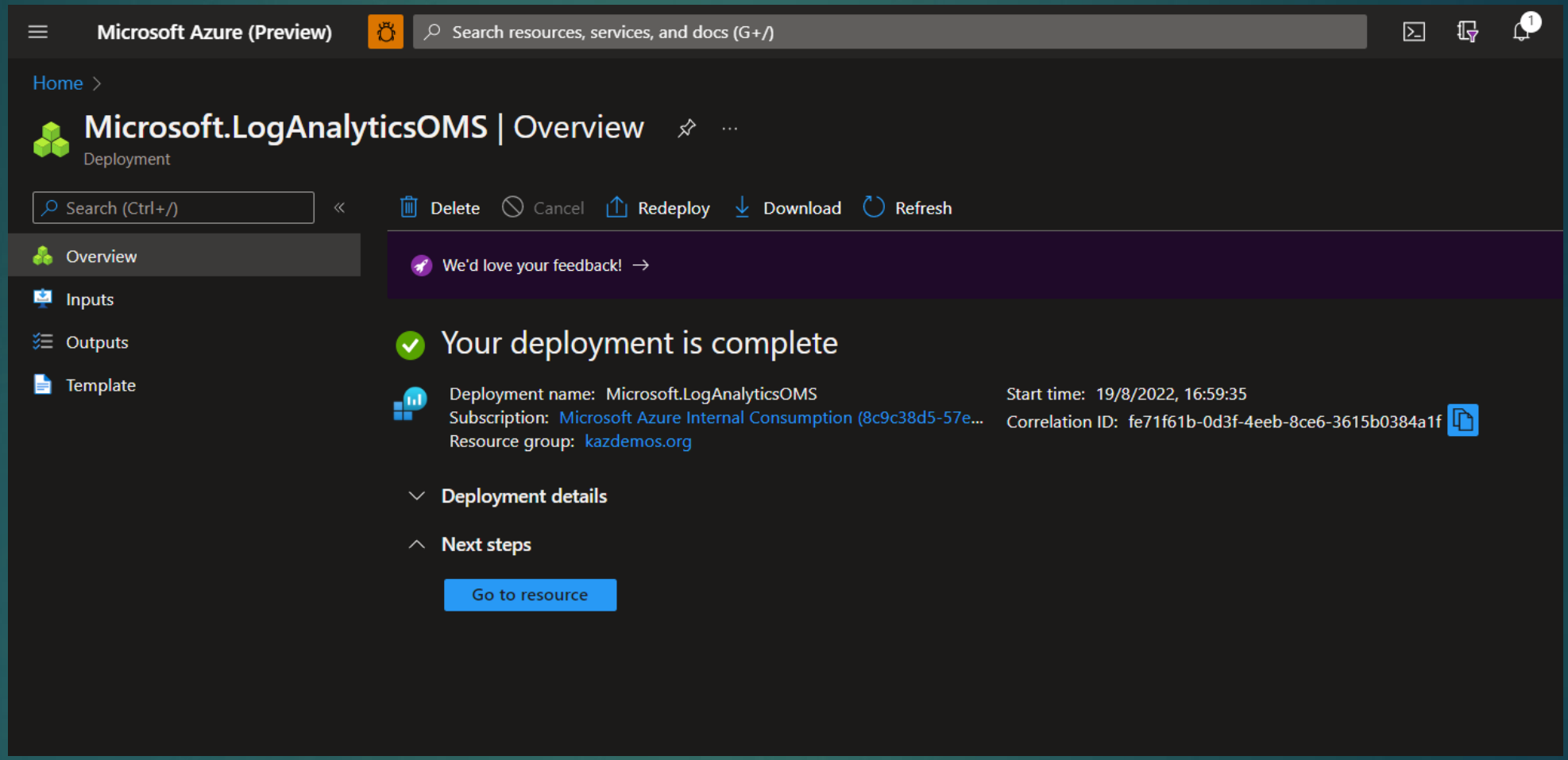
Logs Analytics workspace

Steps



Logs Analytics workspace

Steps

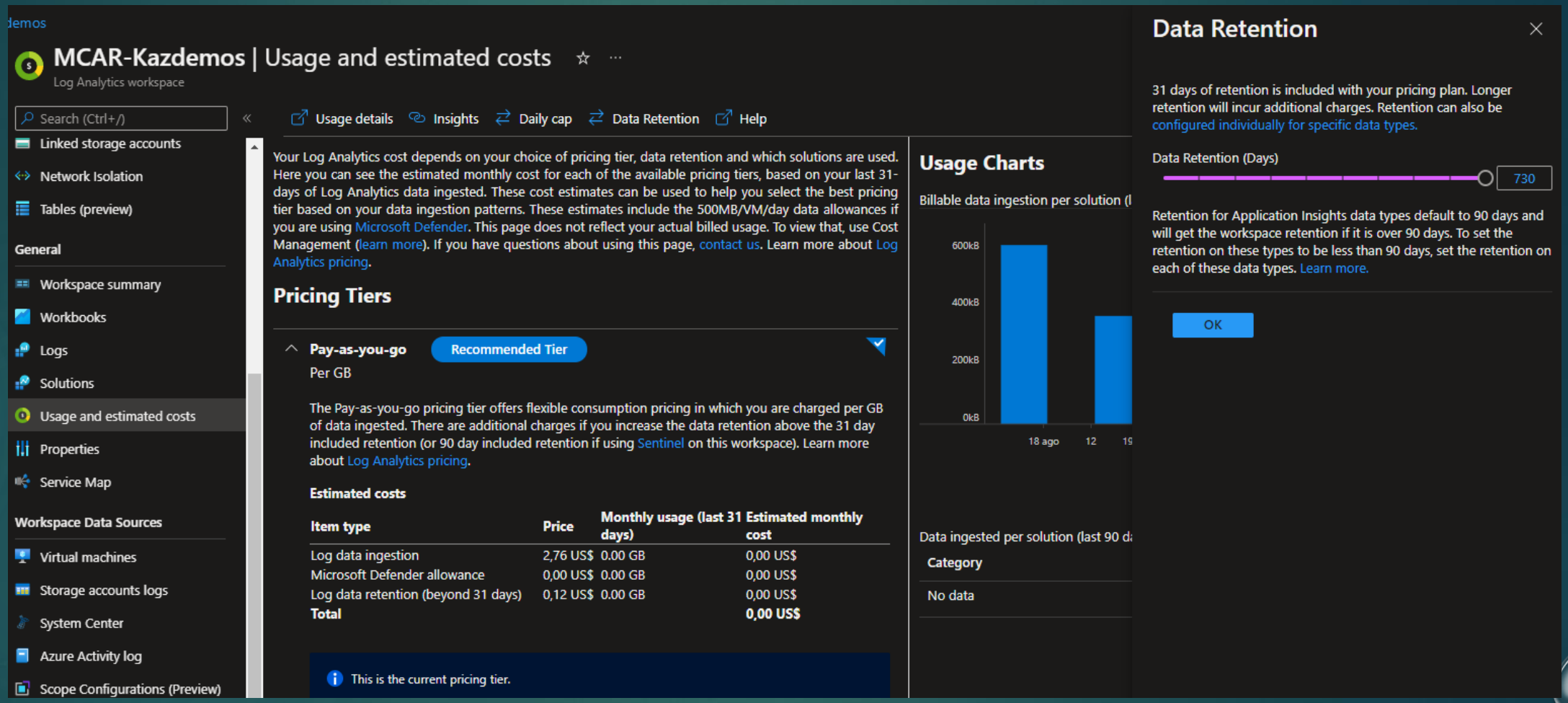


Microsoft

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.



Collect MPARR components

- Open https://aka.ms/MPARR-GitHub
- This site contains all the scripts, guides and templates that we will use in the deployment
- In the root folder a file called "MPARR Collector.zip" can be downloaded with all the scripts, or accessing to MPARR Collector folder each script can be downloaded separately
- Add all the files in a folder in the local drive, as an example c:\MPARR Collector, is not recommended use the files in a synced folder.

MPARR Collector

THIS IS THE LIST ABOUT ALL THE FILES AND FOLDERS THAT YOU NEED FOR MPARR

Certs folder: Certificates created by MPARR_Setup.ps1 will be stored here if you want to backup the certificate in the installation process.

Logs Folder: Here the timestamp.json file is set (this file is used for MPARR_Collector.ps1 script) and additional any error is record here (The default folder is located on C:\APILogs)

RMSLogs Folder: Used by MPARR-RMSData.ps1 script, this is used to process data collected from AIP Service API.

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. This script is created automatically by MPARR_Setup.ps1 script

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. This same file can be used to set the filter capability to "Contains" or "NotContains"

MPARR_Setup.ps1: This is our installation script, is the 1st one that can be executed.

MPARR_Collector.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

MPARR-ExportCSV2LA.ps1: Script used to export the CSV file (located on Support folder) with service plan to Logs Analytics (required to execute on-demand)

MPARR-AzureADUsers.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)

MPARR-AzureADDomains.ps1: Script used to collect data from Azure AD using Microsoft Graph API, permissions are added to Azure AD App for unattended execution, this script permit to collect all the domains registered at Tenant.

MPARR-AzureADRoles.ps1: Script used to collect data from Azure AD using Microsoft Graph API, permissions are added to Azure AD App for unattended execution, this script permit to collect all the administrator roles assigned to user accounts.

MPARR-SITData.ps1: Script used to obtain Display Name and ID for Sensitive Information Types, require ExchangeOnlineManagement PowerShell Module, permissions are added to Azure AD App for unattended execution (can be executed on-demand)

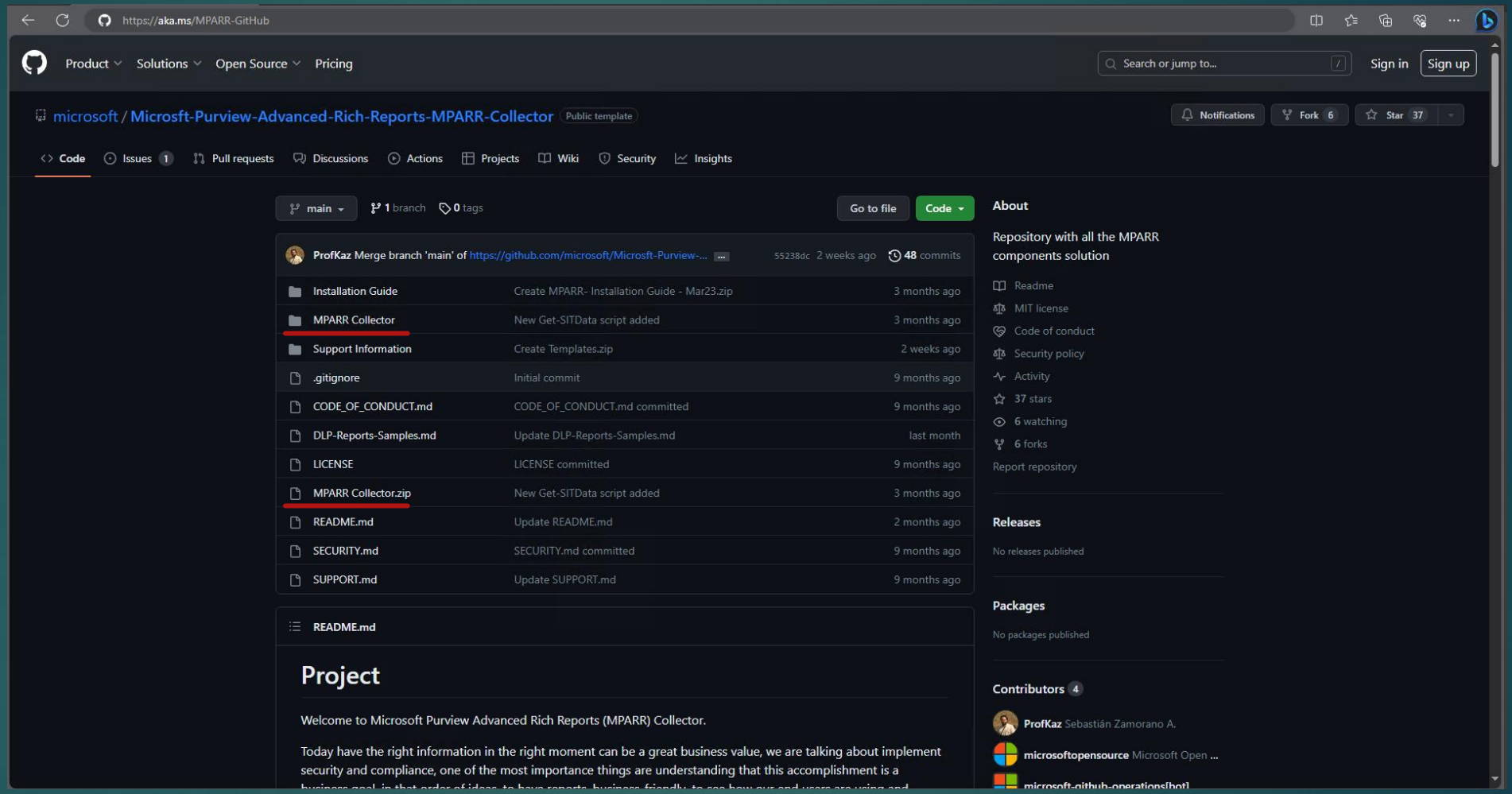
MPARR-LabelData.ps1: Script used to obtain Display Name and ID for labels, require ExchangeOnlineManagement PowerShell Module, permissions are added to Azure AD App for unattended execution (can be executed on-demand)

MPARR-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

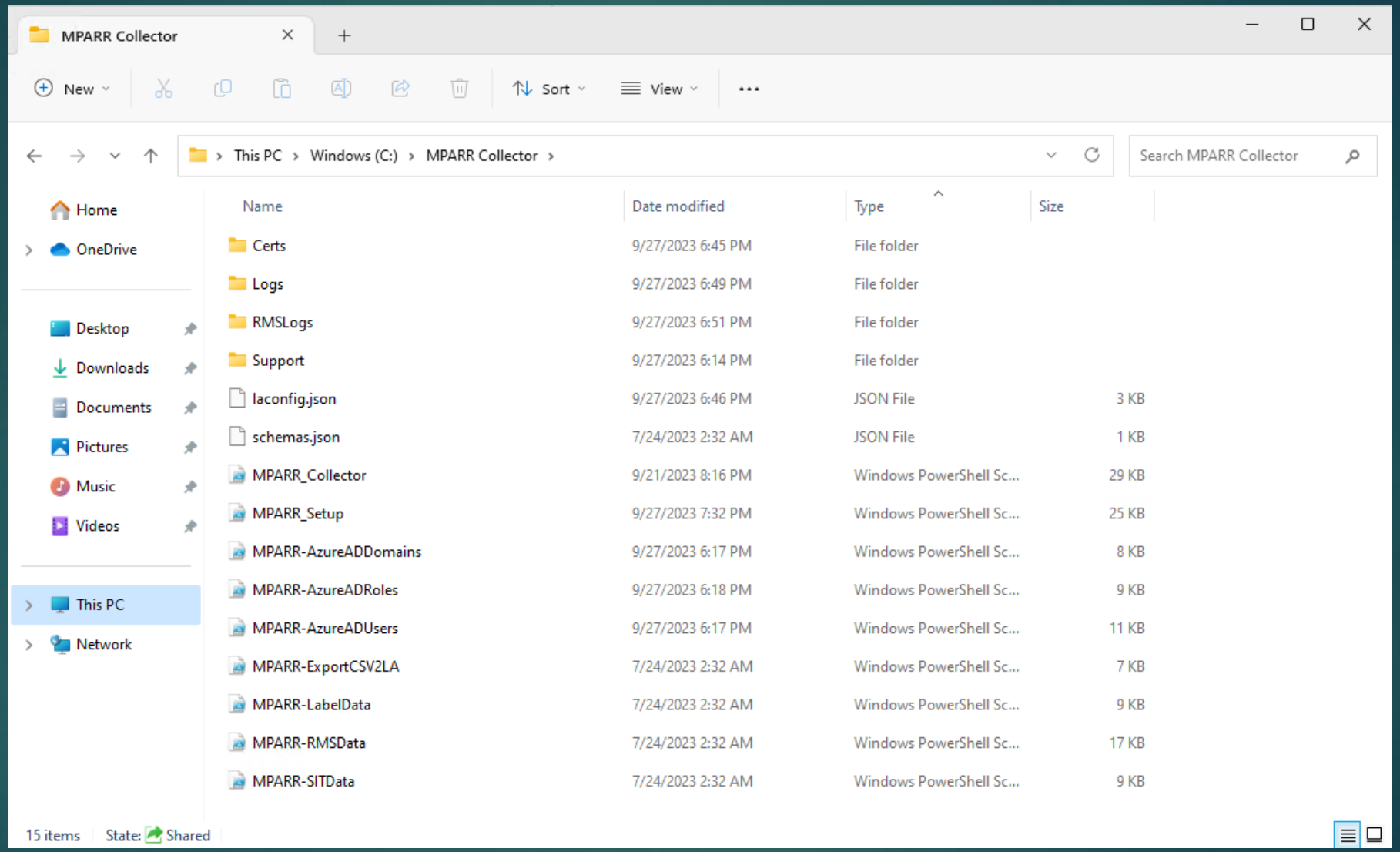
MPARR Collector

Steps



MPARR Collector

Steps



Microsoft

Run MPARR_Setup.ps1

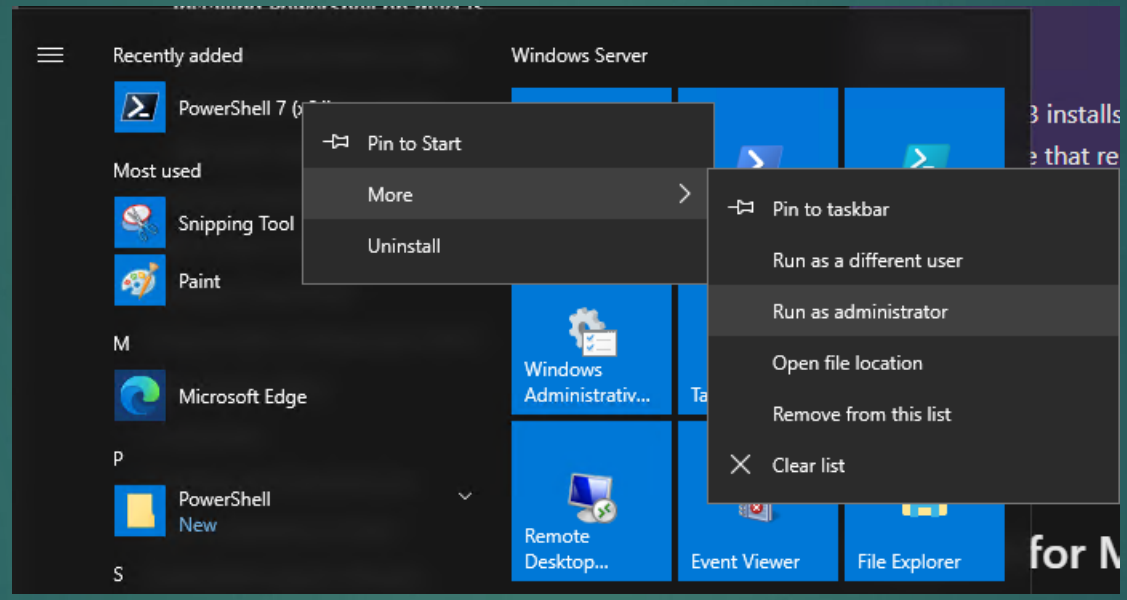
- Open PowerShell 7 with administrator permissions, if you try with the default PowerShell you will receive a message to use the right one and is you try to execute without administrator rights another message appears about use the right permissions.
- Move to the folder that contains all the MPARR files, normally cd 'c:\MPARR Collector\'
- Validate that you have all the folders and files, explained here or shown here.
- Execute .\MPARR_Setup.ps1
  - At the begins the script check if you have all the PowerShell modules needed
  - The script can install all the modules needed, press select Yes
  - Please accept each module to be installed
  - The installer will be automatically exit
- Execute .\MPARR_Setup.ps1 once again
  - First the script will validate that all the modules was correctly installed.
  - Select option 1 to Setup MPARR
    - You'll prompted to add your credentials, you need permissions in your Azure Subscription
    - You will need to select a subscription if you have more than one, you need select the one used to create previously the workspace in Logs Analytics
    - You need to select the right workspace in Logs Analytics

Run MPARR_Setup.ps1 (following previous steps)

- Execute .\MPARR_Setup.ps1 once again (after select the right workspace in Logs Analytics)
  - Select option 1 to Setup MPARR (continuation)
    - You'll prompt for credentials again, in this case to work in Microsoft Entra ID (previously called Azure AD)
    - The Microsoft Entra App will be created with the default name "MPARR-DataCollector", you can accept or change the name
    - A local certificate will be created called "MPARR-DataCollector", you can accept or change the name, this certificate is added to the previous app and is used locally for some of the MPARR scripts, the certificate is installed locally at the same time
    - You can select for how many time that you want to set the certificate, by default is 12 months and can be extended for 36 months
    - Now you can decide if you want to backup the certificate, in that case the certificate is stored under Certs folder, and you will be prompted to set a password for the PFX file.
    - A secret key will be created, and you can change the name used for the description, this key is created on the same Microsoft Entra App
    - You need to select your kind of Tenant between Commercial, GCC, GCCH, or DoD, by default is Commercial
    - MPARR_Collector.ps1 and MPARR-RMSData.ps1 uses some logs and supporting files, like a timestamp, to manage the data that is collected and imported to Logs Analytics, you need to select the folders for each one, is recommend select the empty folders located on the original "MPARR Collector.zip", those folders are located on the same path of this script and are Logs for MPARR_Collector and RMSLogs for MPARR-RMSData
    - Please select the right folder in each case and press the button select folder
  - Select option 2 to encrypt the keys stored in the configuration file called "laconfig.json", all the previous configuration is stored in that file and considering security the passwords can be hashed using the local machine ID and the user logged.
  - Select option 3 to create 2 tasks in the task scheduler to execute automatically every 15 minutes MPARR_Collector and MPARR_RMSData scripts.
  - Select option 0 to exit, is almost done, please check in the next section the latest steps to finish

MPARR Collector

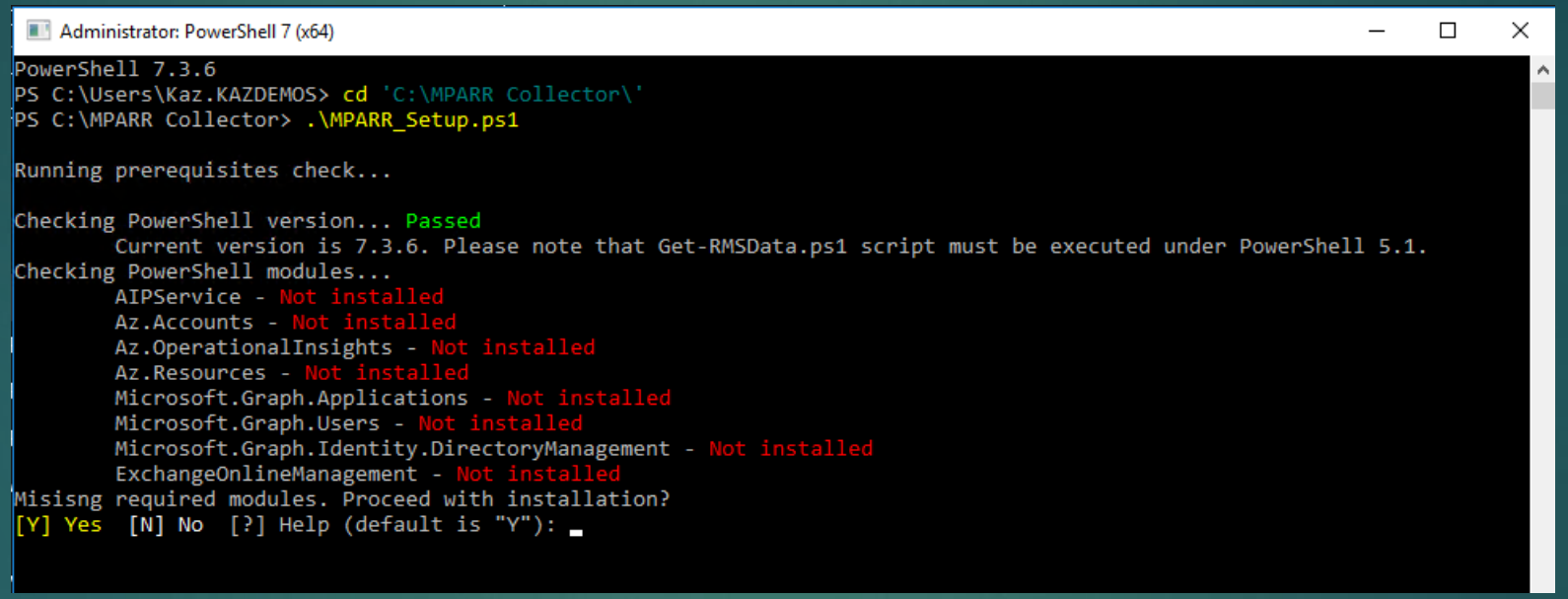
Steps



Microsoft

MPARR Collector

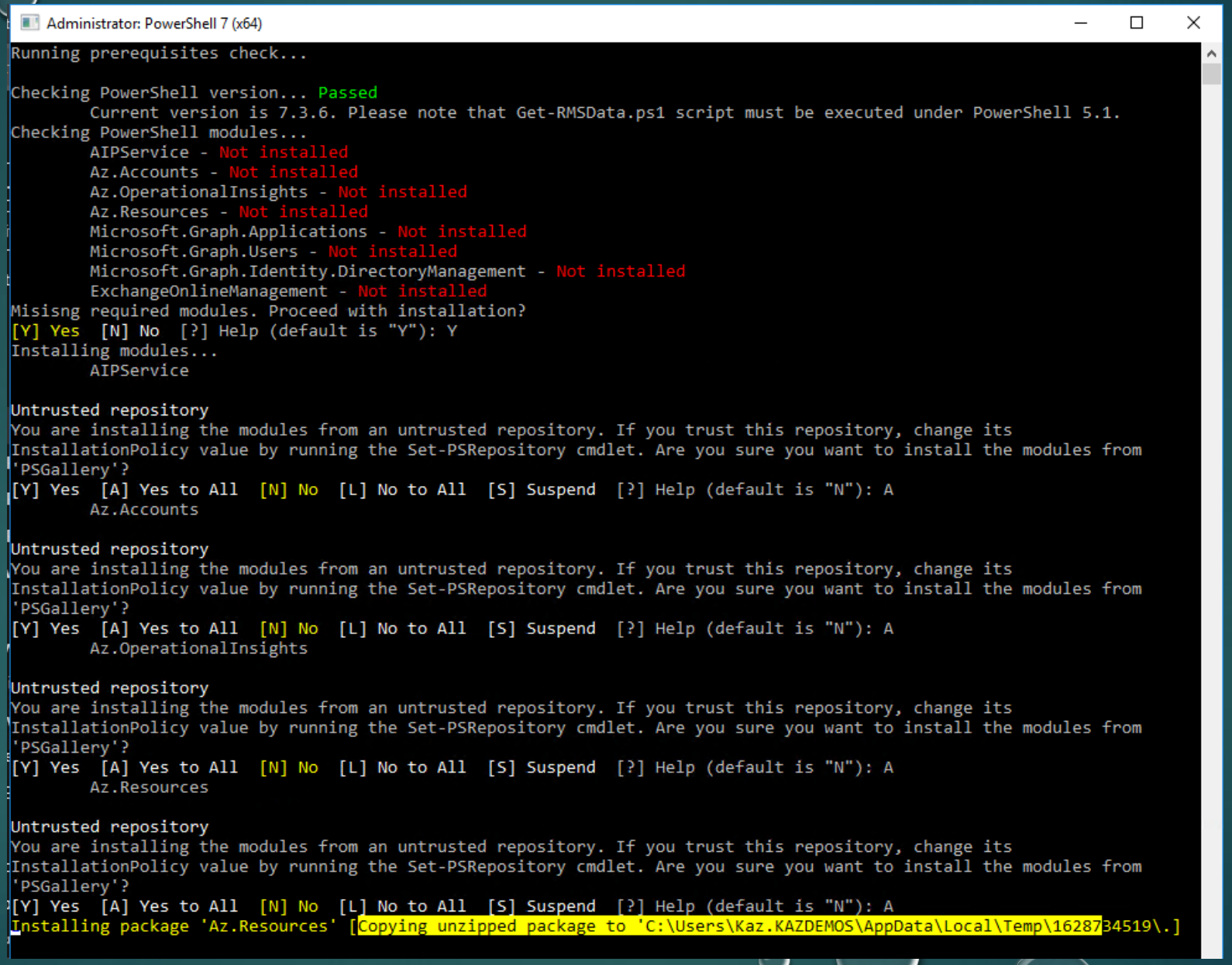
Steps



Microsoft

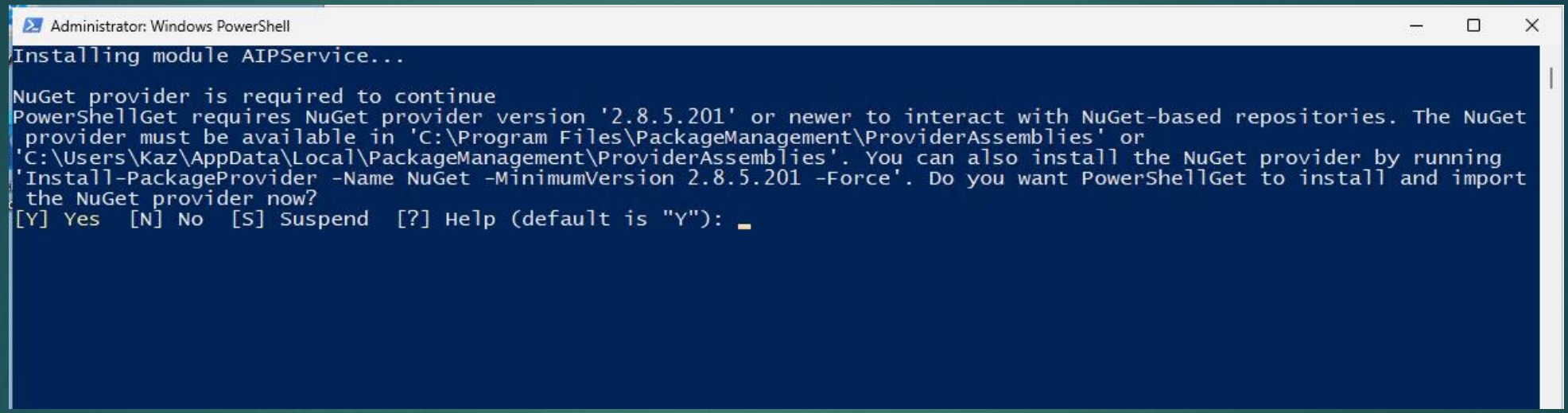
MPARR Collector

Steps



MPARR Collector

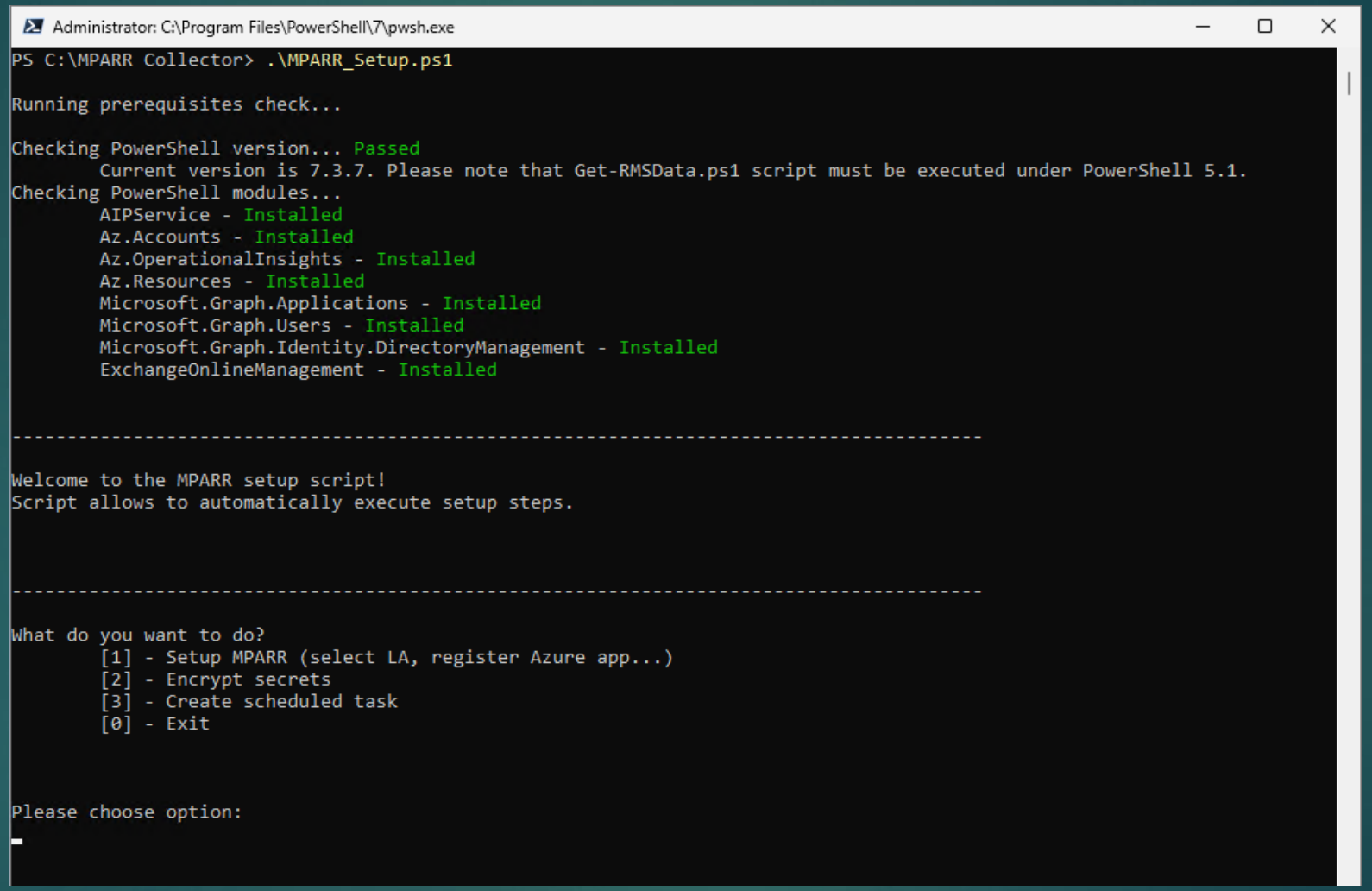
Steps



Microsoft

MPARR Collector

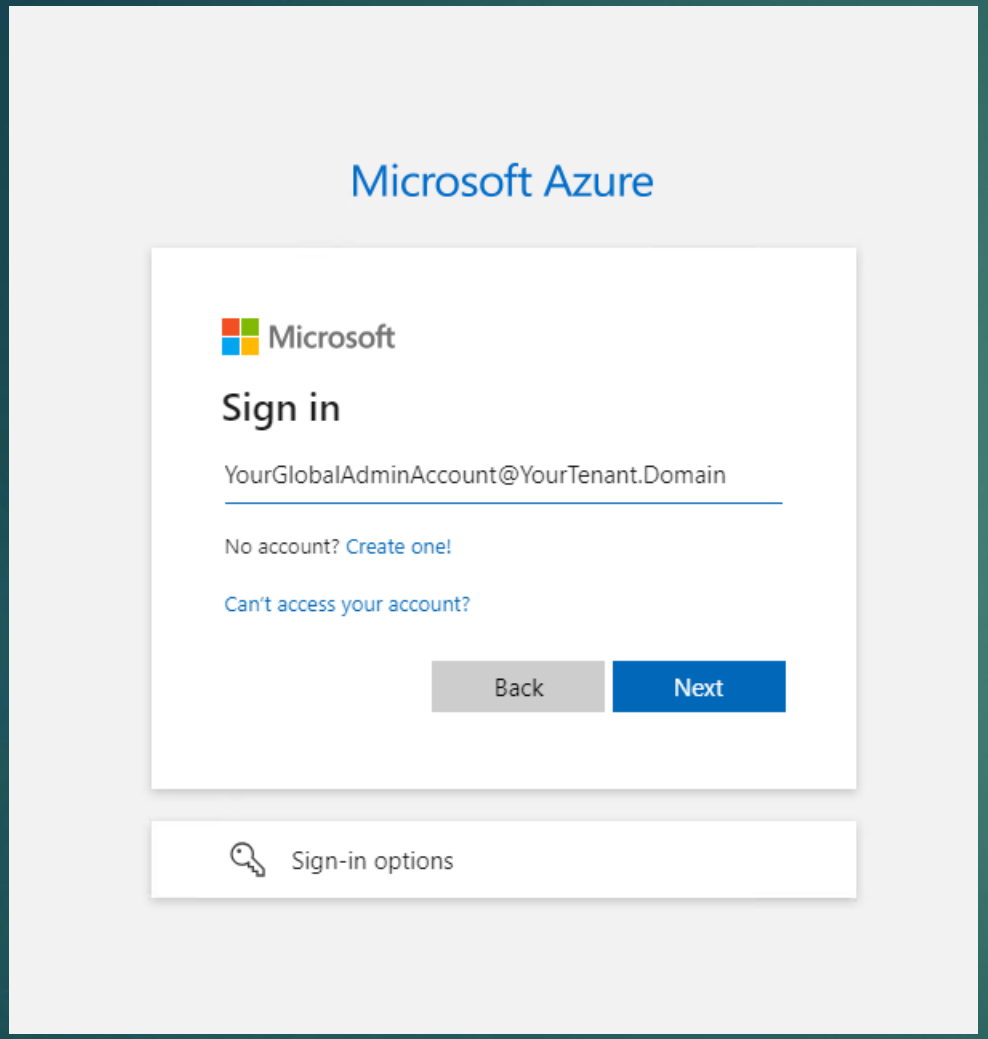
Steps

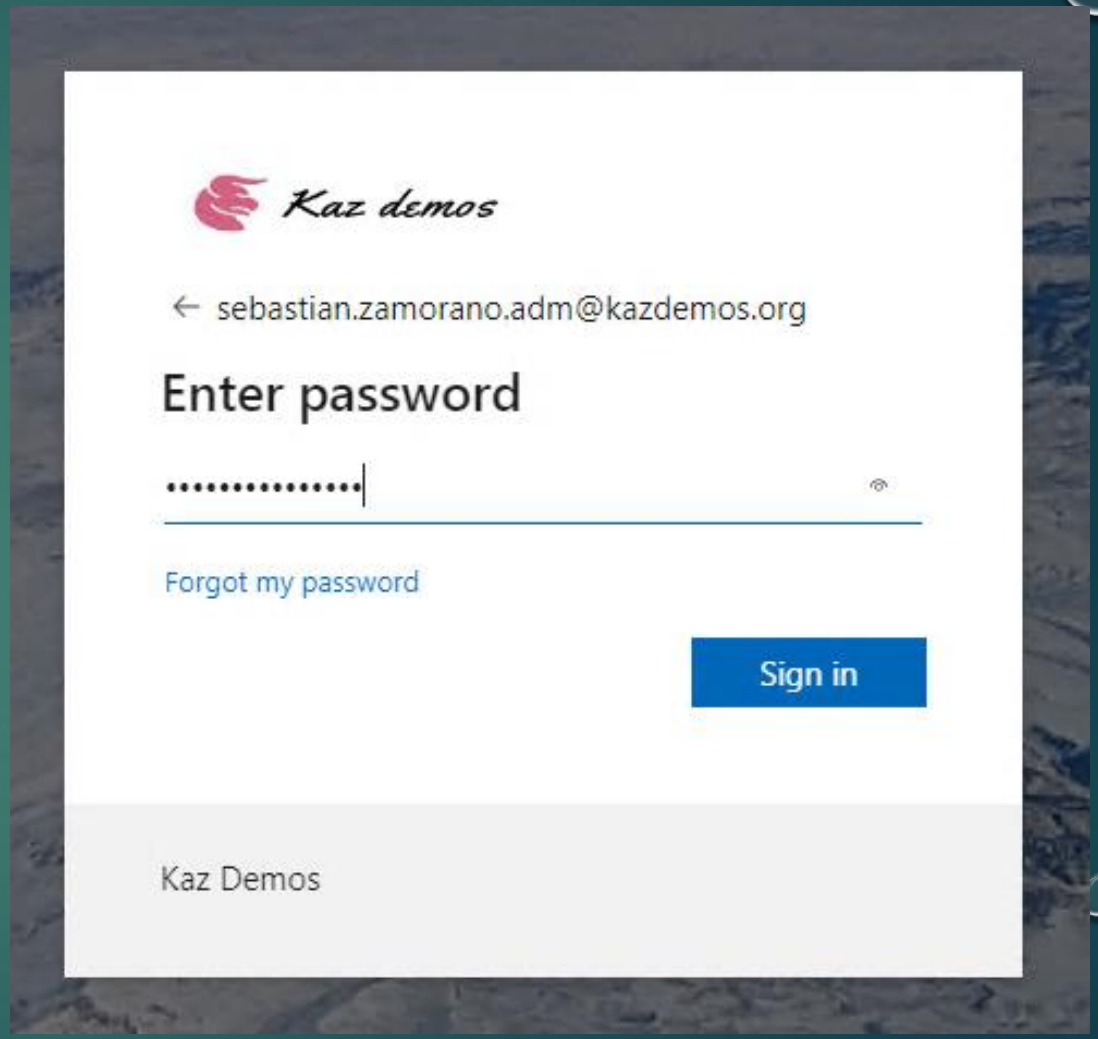


Microsoft

MPARR Collector

Steps





Microsoft

MPARR Collector

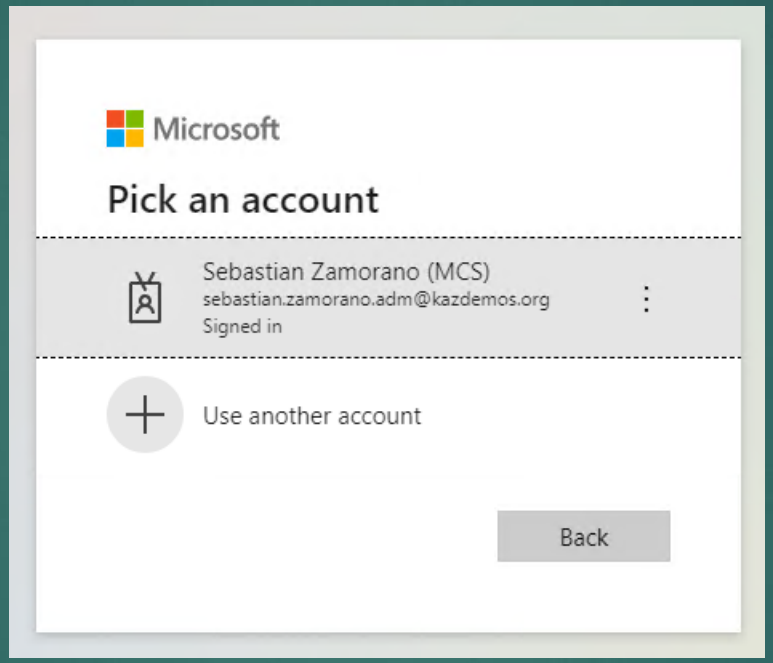
Steps

```
Getting subscriptions...

No Name                      Id
-- ----                      --
 1 Visual Studio Enterprise 2e3c2e66-e9f7-4ebe-91e5-599c09ab2ad8
 2 Azure Pass - Sponsorship f4841c1d-23ed-4ccd-9828-cc3023bf2f57

Enter number corresponding to the subscription: 2

Name                                  Account            SubscriptionName    Environment        TenantId
----                                  -------            ----------------    -----------        --------
Azure Pass - Sponsorship (f4841c1d-23ed… sebastian.zamorano… Azure Pass - Spons… AzureCloud         ac1dff03-7e0e-4ac…

Getting workspaces...

No Name          ResourceGroupName Location Sku       Tags
-- ----          ----------------- -------- ---       ----
 1 MPARR         mparr-demo        eastus   pergb2018 {}
 2 MPARR-Kazdemo mparr-demo        eastus   pergb2018 {}
 3 MPARRData     mparr-demo        eastus   pergb2018 {}

In case workspace recently created is not listed, please stop the script with Ctrl+C and run it again.

Enter number corresponding to the Log Analytics workspace: _
```

Microsoft

MPARR Collector

Steps



Microsoft

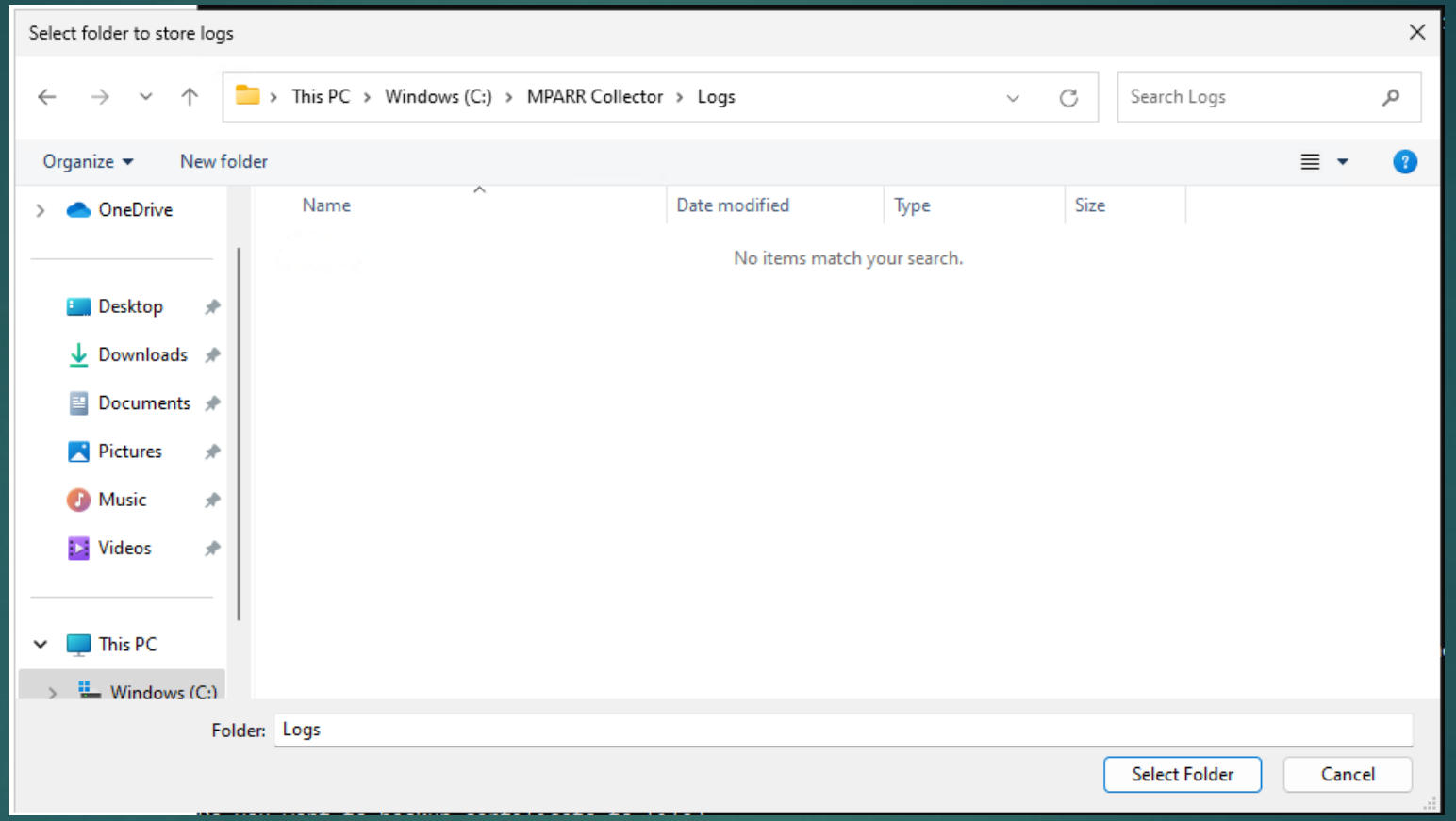
MPARR Collector

Steps

```
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

'MPARR-DataCollector' app already exists. New name was generated: 'MPARR-DataCollector-be51d51f'

'MPARR-DataCollector-be51d51f' application will be registered. Do you want to proceed or change the name?
[P] Proceed  [C] Change  [?] Help (default is "P"): C
Please enter the new name: MPARR-Data
Default certificate name is 'MPARR-DataCollector'. Do you want to proceed or change the name?
[P] Proceed  [C] Change  [?] Help (default is "P"):
Certificate is valid for 12 months. Do you want to change this value?
[Y] Yes  [N] No  [?] Help (default is "N"):
Do you want to backup certificate to file?
[Y] Yes  [N] No  [?] Help (default is "N"): Y
Please enter password to secure certificate: ***************
Default client secret name is 'Secret1'. Do you want to proceed or change the name?
[P] Proceed  [C] Change  [?] Help (default is "P"):

Azure application was created.
App Name: MPARR-Data
App ID: 2e1f21b0-d435-46c0-b0d8-3fd846b49b8f
Secret password: pbJ8Q~4fP6y7FLiiGydYuGe_~iQZX_FHqGeqOcuV
Certificate thumbprint: D4A580C5035851E847160E22249801319D9B58D5

Please go to the Azure portal to manually grant admin consent:
https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/appId/2e1f21b0-d435-46c0-b0
d8-3fd846b49b8f


Please select cloud version:
[C] Commercial  [G] GCC  [H] GCCH  [D] DOD  [?] Help (default is "C"):
```

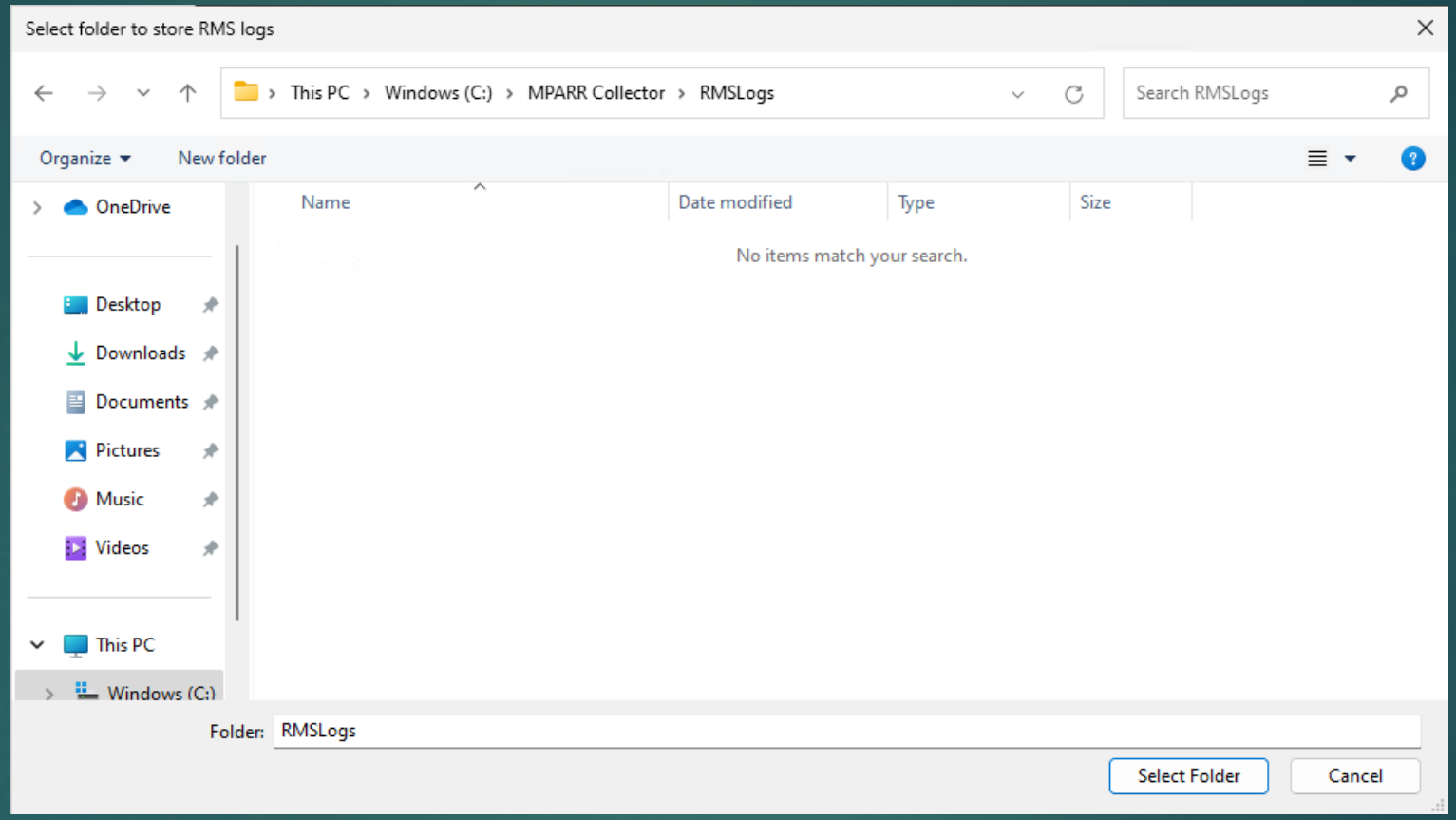
MPARR Collector

Steps



MPARR Collector

Steps



Microsoft

MPARR Collector

Steps

```
Default locations for logs are 'c:\APILogs\RMSLogs\' and 'c:\APILogs\'. Do you want change the location?
[Y] Yes  [N] No  [?] Help (default is "N"): Y

Output logs set to 'C:\MPARR Collector\Logs\'.

RMS logs set to 'C:\MPARR Collector\RMSLogs\'.
Setup completed. New config file was created.
```

Microsoft

MPARR Collector

Steps

```
--------------------------------------------------------------------------------

What do you want to do?
        [1] - Setup MPARR (select LA, register Azure app...)
        [2] - Encrypt secrets
        [3] - Create scheduled task
        [0] - Exit



Please choose option:

Secrets encrypted.
The old config file moved to 'laconfig_20230928040039.json'
Warning!
Please note that encrypted keys can be decrypted only on this machine, using the same account.
```

Microsoft

MPARR Collector

Steps

laconfig.json

```
{
  "EncryptedKeys": "False",
  "AppClientID": "2e1f21b0-d435-46c0-b0d8-3fd846b49b8f",
  "ClientSecretValue": "p[redacted]",
  "TenantGUID": "acldff03-7e0e-4ac8-a4c9-9b38d24f062c",
  "TenantDomain": "kazdemos.org",
  "LA_CustomerID": "87aab88e-b962-4dfc-aff6-d960d19ac360",
  "LA_SharedKey": "1t[redacted]",
  "CertificateThumb": "D[redacted]",
  "OnmicrosoftURL": "M365x089236.onmicrosoft.com",
  "RMSLogs": "C:\\MPARR Collector\\RMSLogs\\",
  "OutPutLogs": "C:\\MPARR Collector\\Logs\\",
  "Cloud": "Commercial"
}
```

laconfig.json

```
{
  "EncryptedKeys": "True",
  "AppClientID": "2e1f21b0-d435-46c0-b0d8-3fd846b49b8f",
  "ClientSecretValue": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c500000000002
  "TenantGUID": "acldff03-7e0e-4ac8-a4c9-9b38d24f062c",
  "TenantDomain": "kazdemos.org",
  "LA_CustomerID": "87aab88e-b962-4dfc-aff6-d960d19ac360",
  "LA_SharedKey": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c5000000000200000
  "CertificateThumb": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c500000000020
  "OnmicrosoftURL": "M365x089236.onmicrosoft.com",
  "RMSLogs": "C:\\MPARR Collector\\RMSLogs\\",
  "OutPutLogs": "C:\\MPARR Collector\\Logs\\",
  "Cloud": "Commercial"
}
```

Microsoft

MPARR Collector

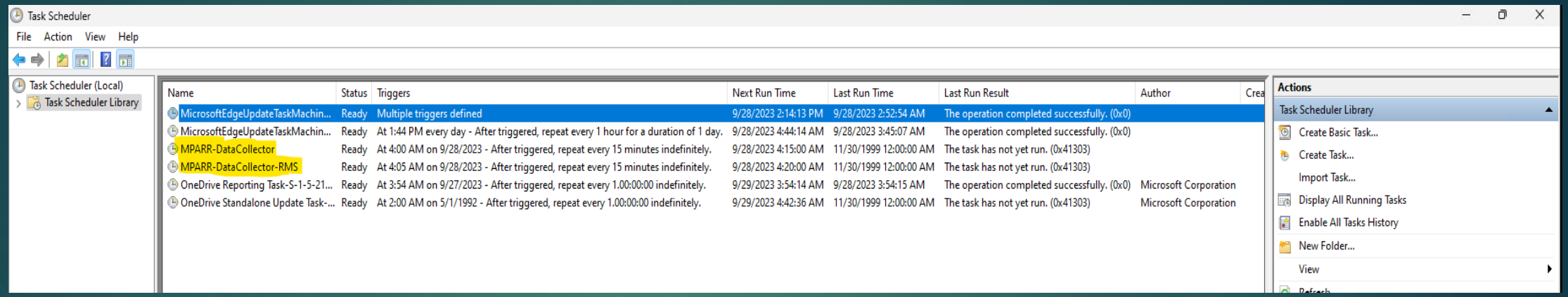
Steps

```
--------------------------------------------------------------------------------

What do you want to do?
        [1] - Setup MPARR (select LA, register Azure app...)
        [2] - Encrypt secrets
        [3] - Create scheduled task
        [0] - Exit



Please choose option:

Scheduled task named 'MPARR-DataCollector' was created.
For security reasons you have to specify run as account manually.


Scheduled task named 'MPARR-DataCollector-RMS' was created.
For security reasons you have to specify run as account manually.
```

Microsoft

MPARR Collector

Steps



Microsoft

MPARR Setup final steps

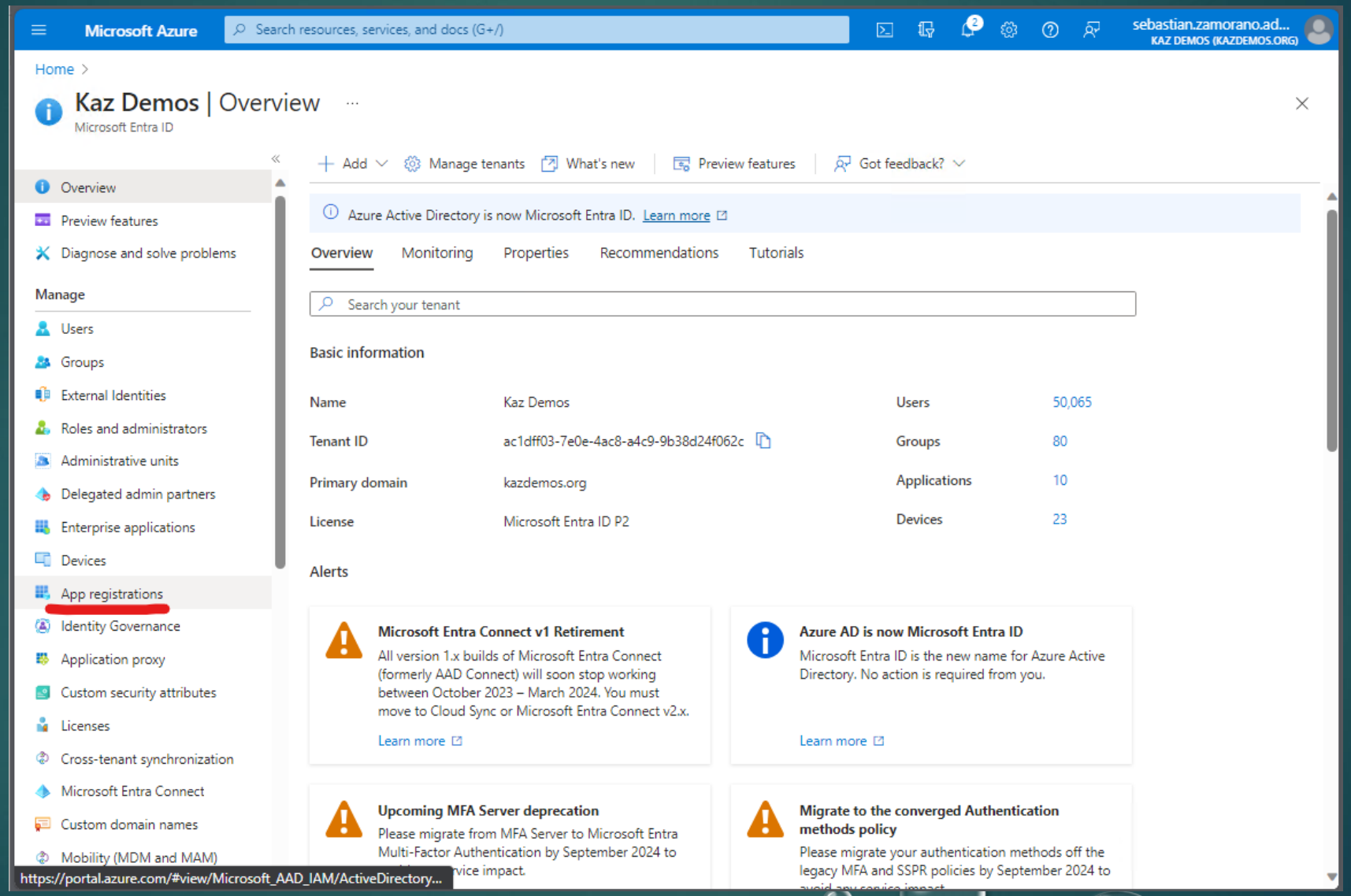
Some latest steps to finish MPARR configuration

- To finish the MPARR Collector installation we need to do this steps:
  - To enable the API permissions is required open Microsoft Entra ID
    - Go to https://portal.azure.com and search for Microsoft Entra ID and select
    - Search for App registrations and select
    - In the new pane please look for your new App created, normally called MPARR-Datacollector and select it
    - In the new interface in the left menu select API permissions
    - And we need to grant admin consent, all the APIs used appears with a warning triangle, after you grant the permissions all we be put on green, you need to select Yes to apply.
    - Close the Configuration
  - At task scheduler we need to give permissions to the tasks to run without a logged user, to do that we need to do the next steps:
    - Check that the tasks are working selecting each one and pressing run
    - In some case an advice can appears related to the scripts, needing to unblock the file to be used
      - Under PowerShell is required execute PS C:\MPARR Collector> **Unblock-File .\MPARR-RMSData.ps1**
    - The tasks are set to run every 15 minutes indefinitely, this time can be changed and affect the time to takes to update the data in Logs Analytics
    - Each task are created to use the current logged on user but is recommend to change to "Run whether user is logged on or not", local account credentials will be required after change this configuration and press OK.
  - **Now enjoy MPARR**

Microsoft

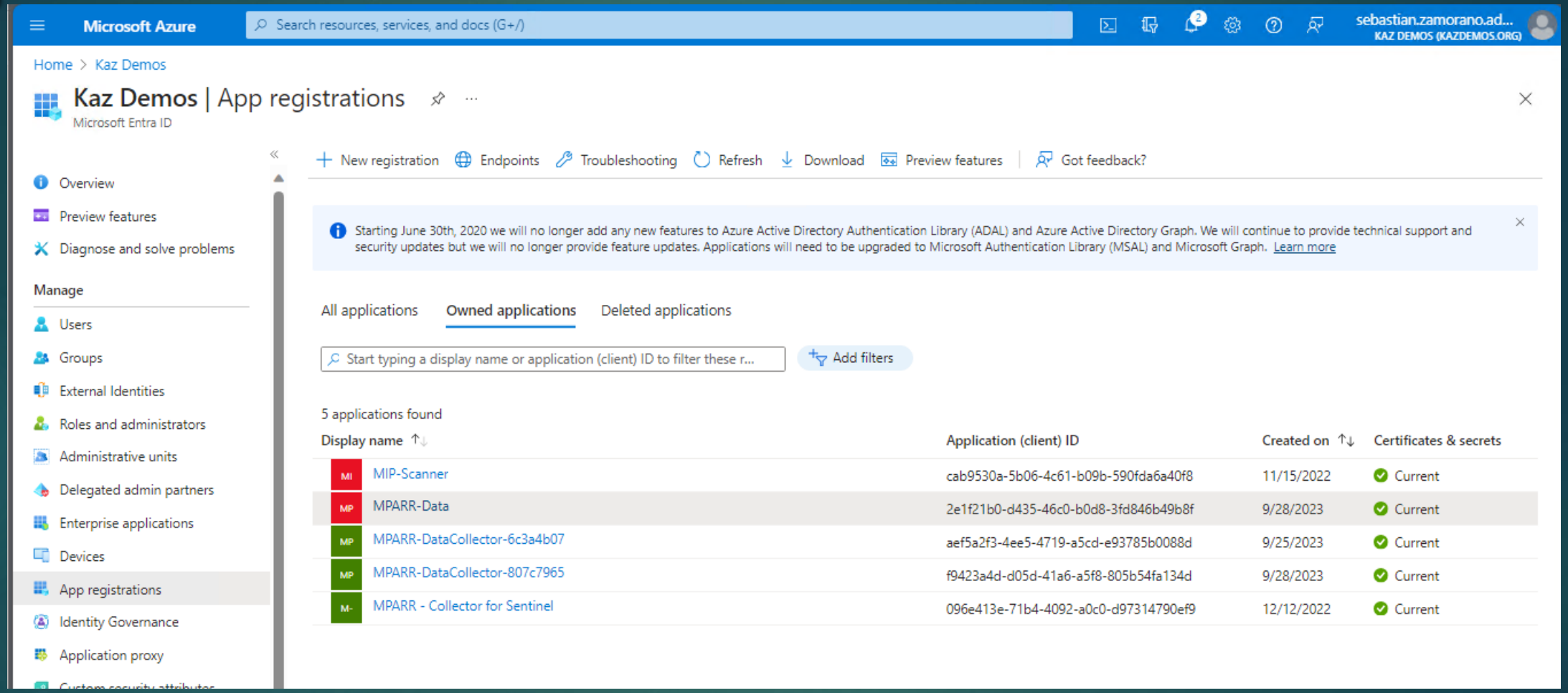
MPARR Setup final steps

Steps



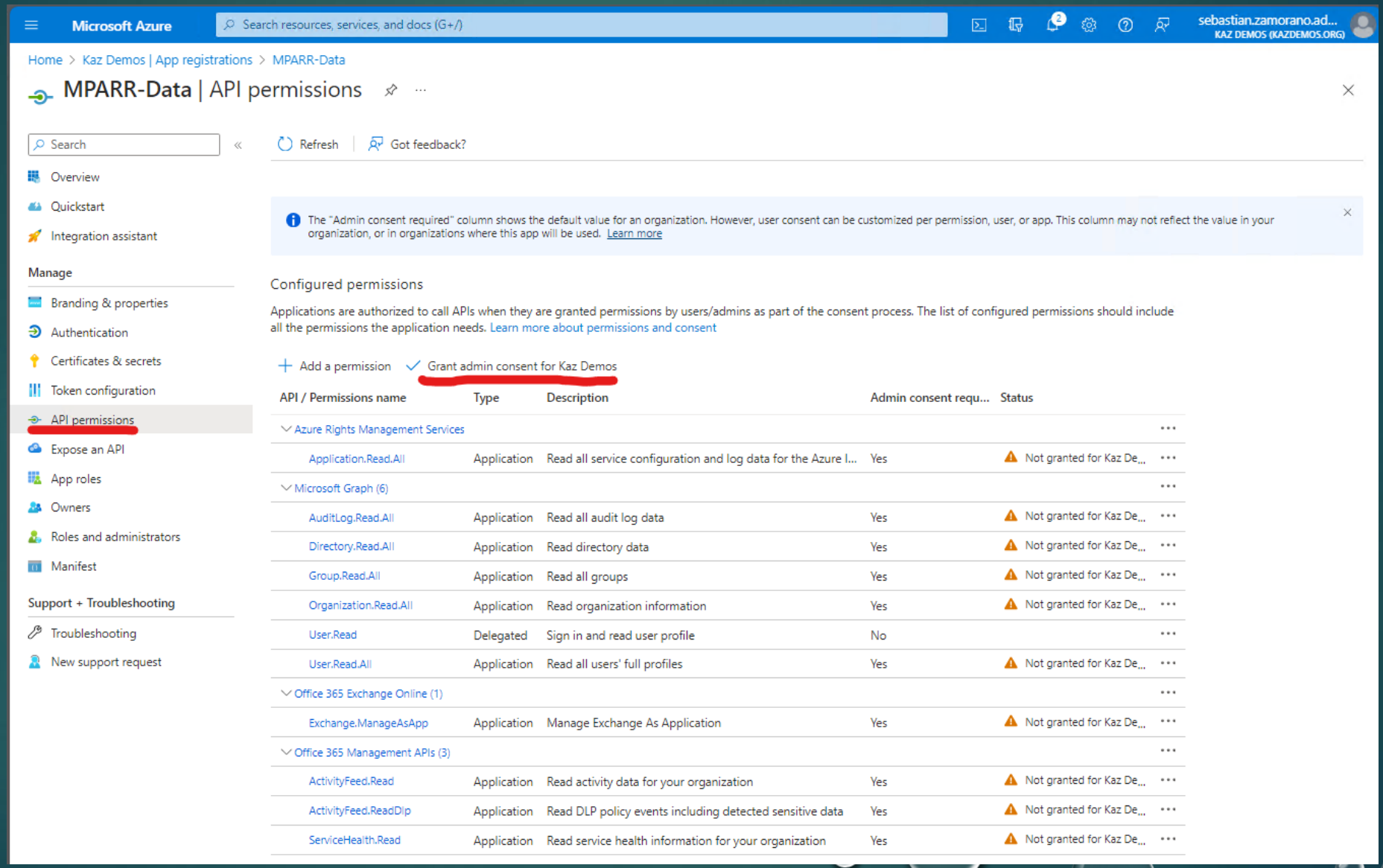
Steps

MPARR Setup final steps



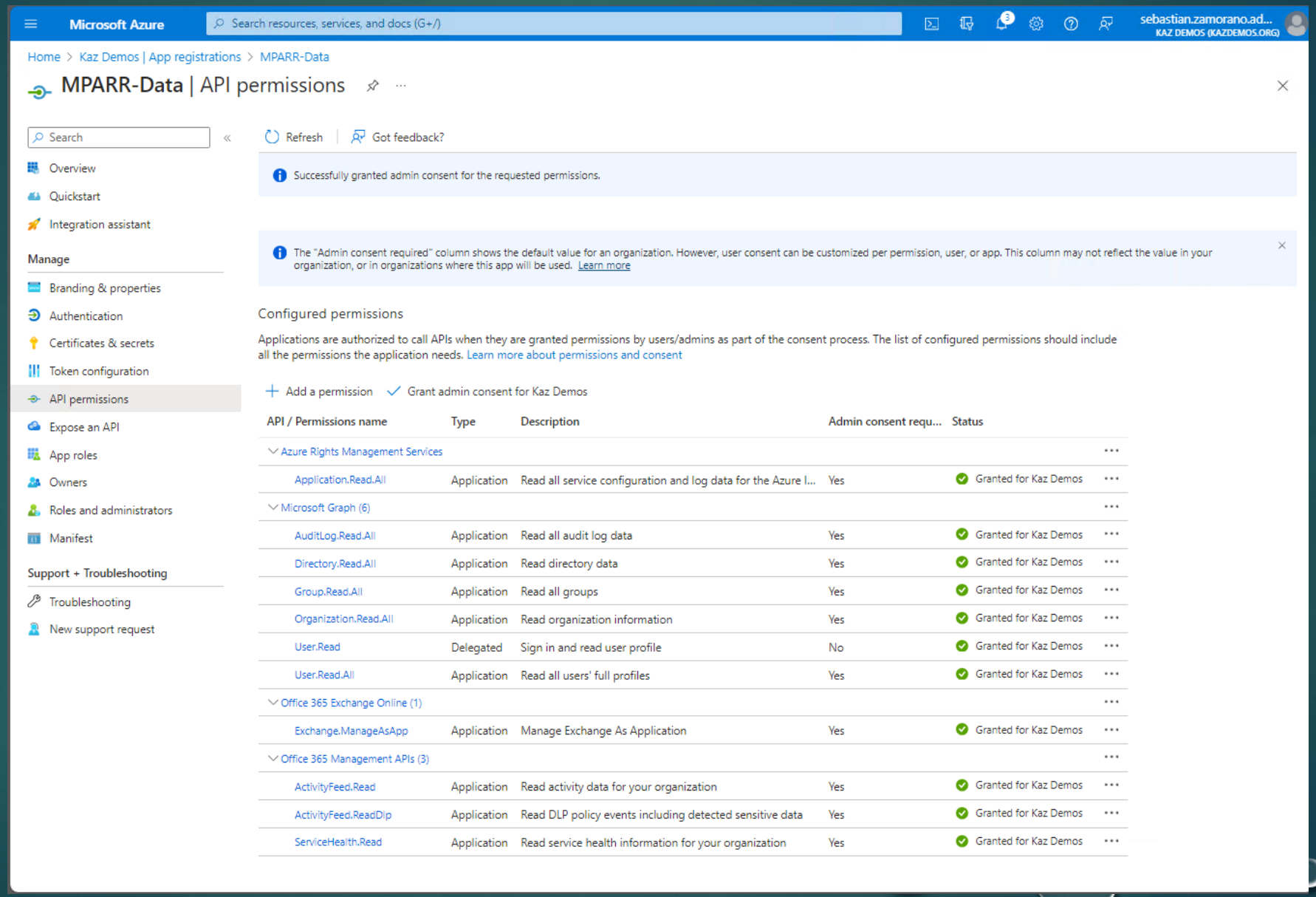
MPARR Setup final steps

Steps



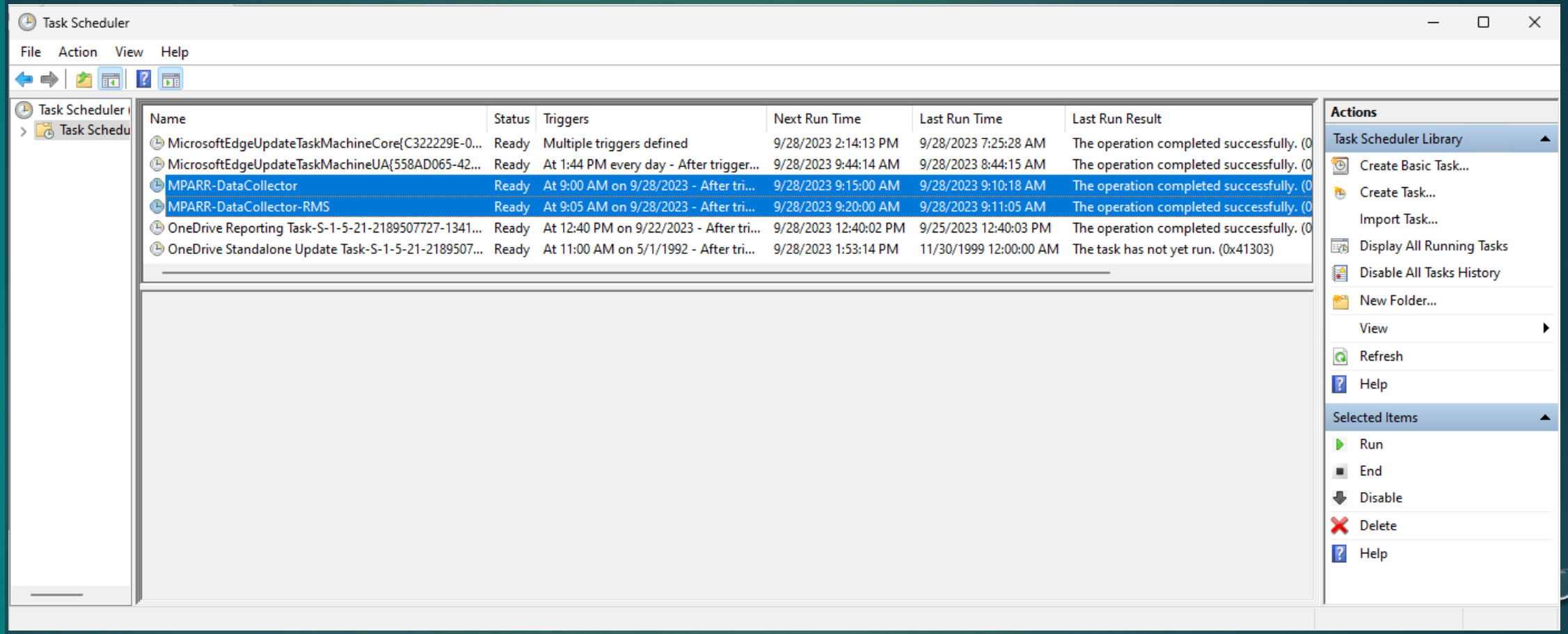
MPARR Setup final steps

Steps



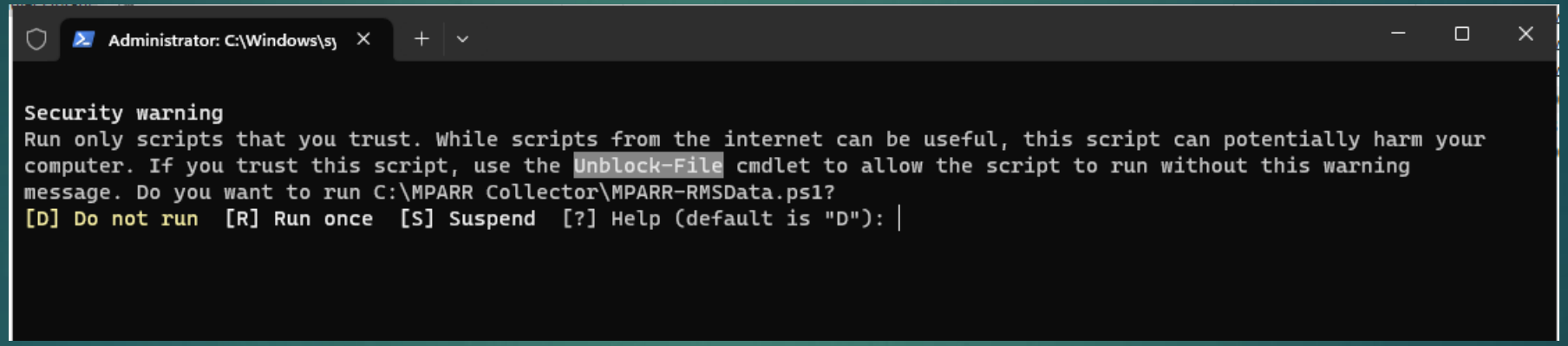
MPARR Setup final steps

Steps



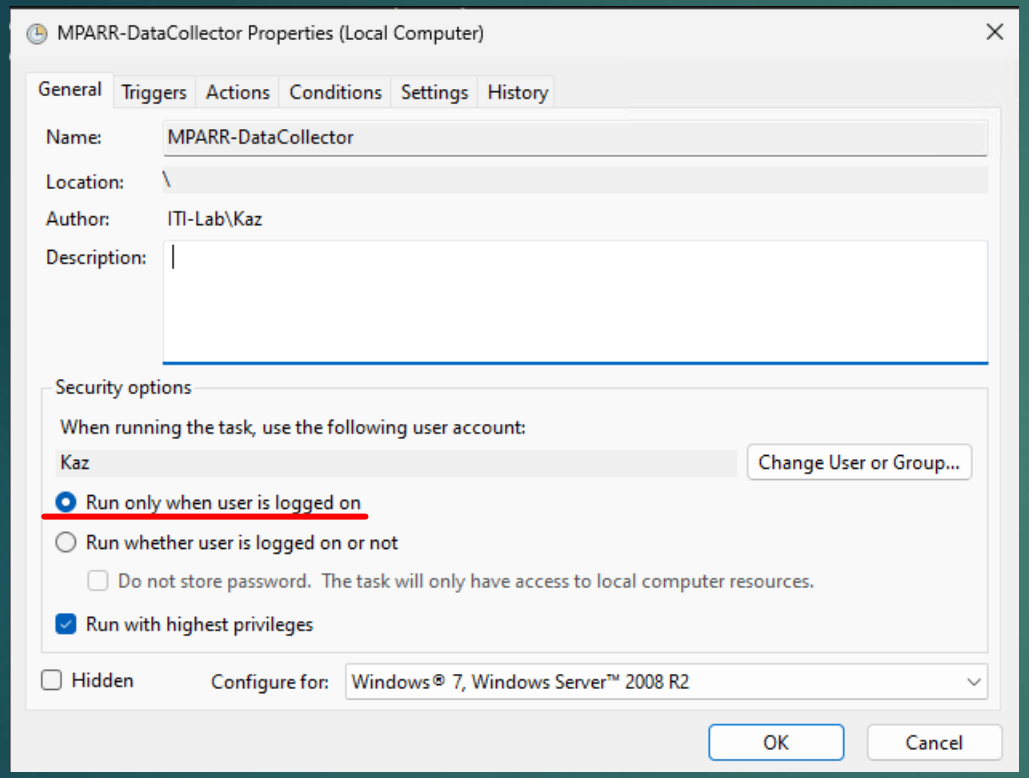
MPARR Setup final steps

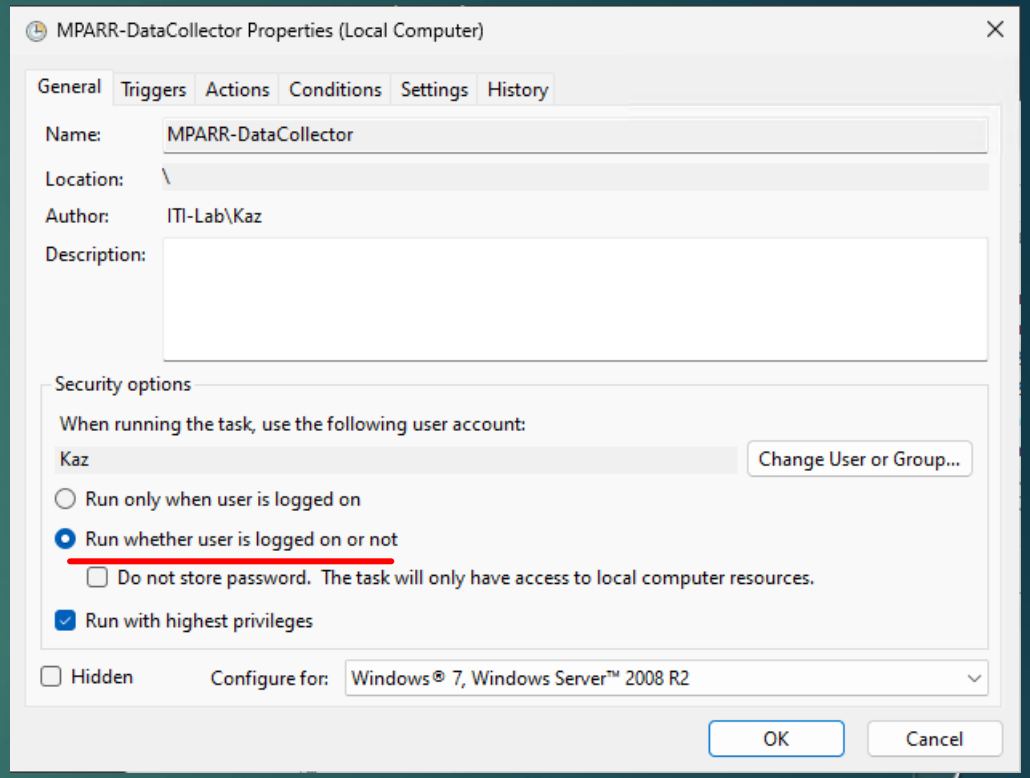
Steps



MPARR Setup final steps

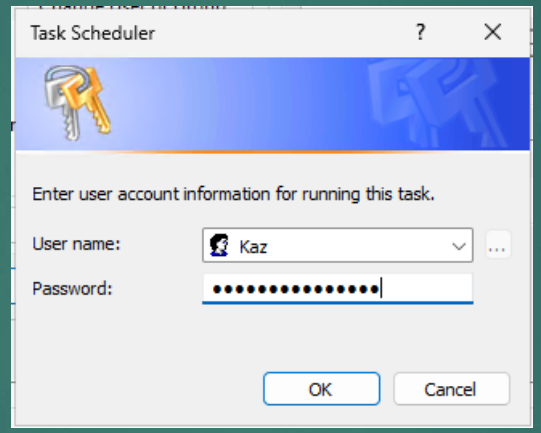
Steps





MPARR Setup final steps

Steps



Compliance Admin Role for Script

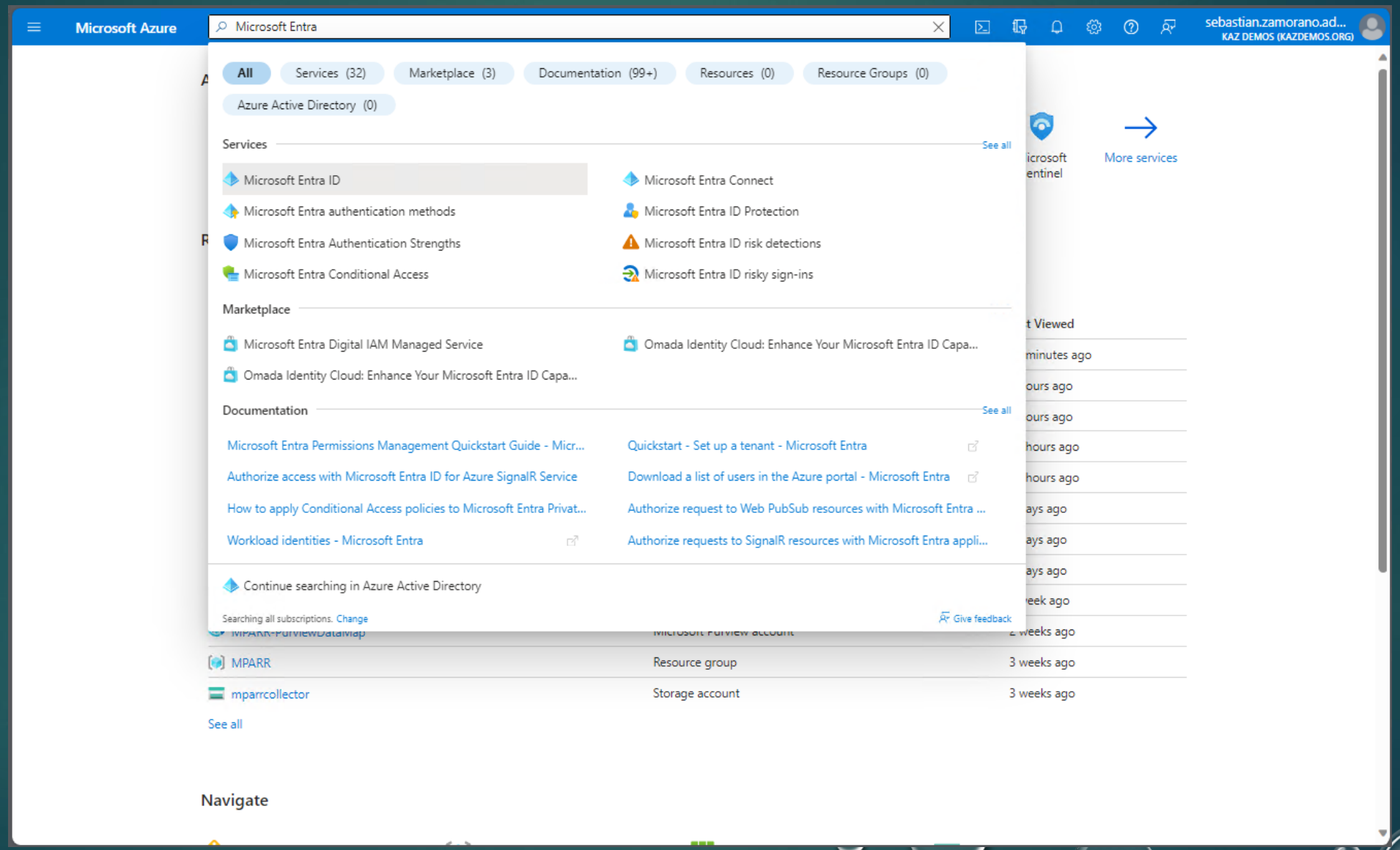
Compliance administrator role assigned to Azure AD App

- To execute MPARR-LabelData.ps1 and MPARR-SITData.ps1 scripts additional permissions are required to the previously App created:
  - To give the permissions is required open Microsoft Entra ID
  - 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 Microsoft Entra App previously created, normally called MPARR-DataCollector, 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
- Understanding the complexity to give elevate privileges to an unattended script, a line can be modified on the script to a manual execution, in this case someone with Compliance Administrator role needs to execute this script on PowerShell, this execution is on-demand and is required only when you have modified labels or new labels, to up to date the reports with this information, or can be required depending the retention period in the Logs Analytics workspace.

Microsoft

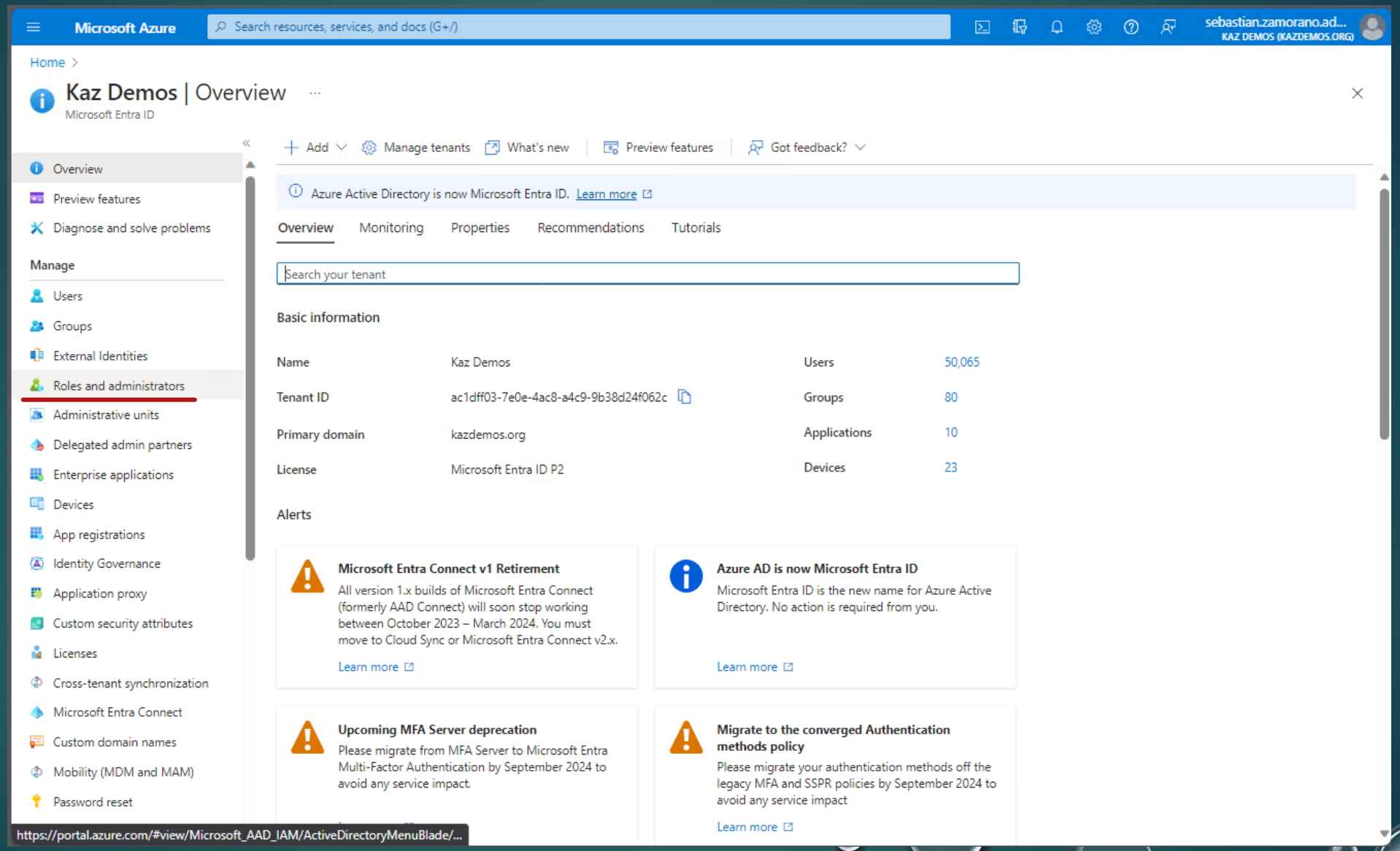
Compliance Admin Role for Script

Steps



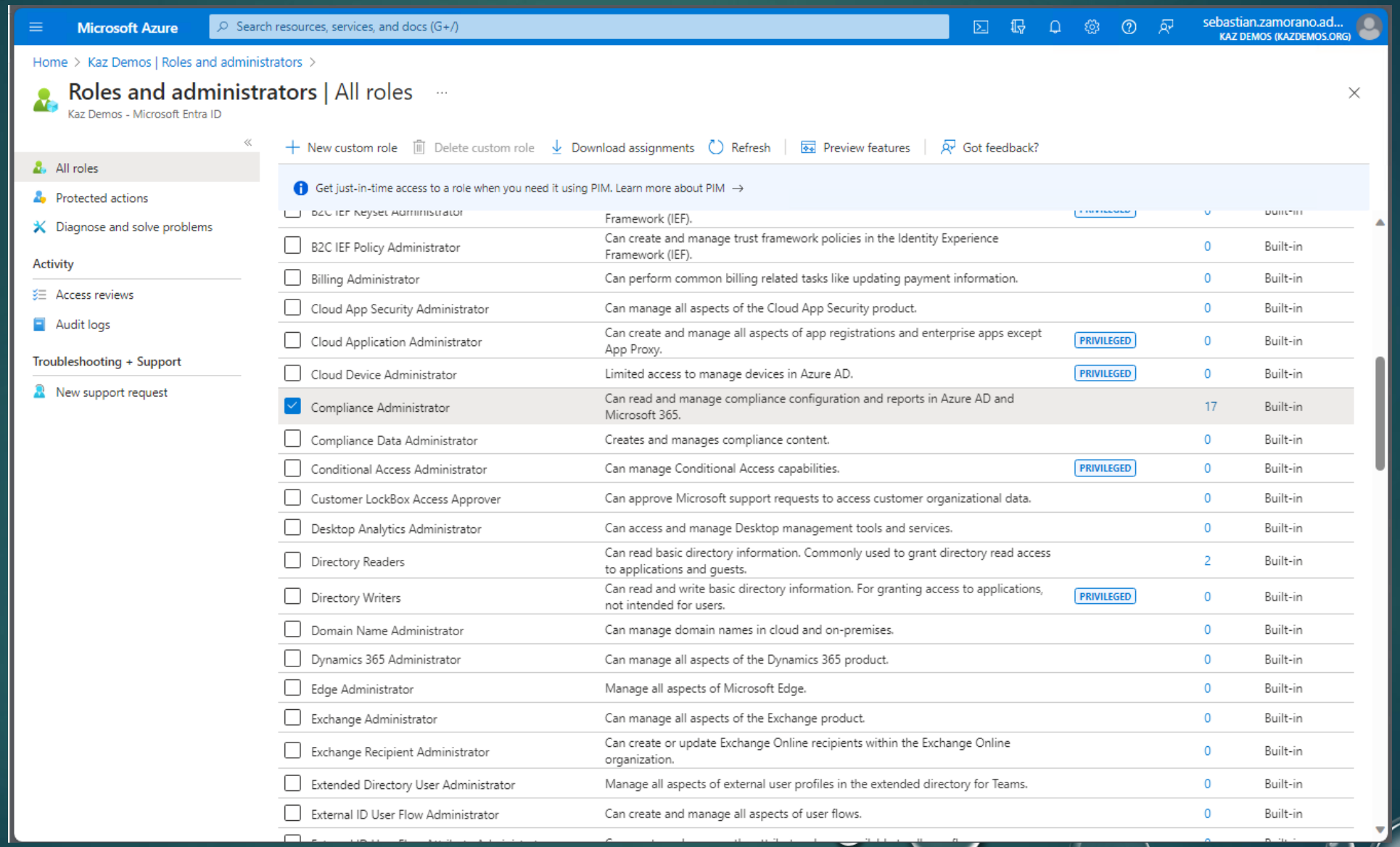
Compliance Admin Role for Script

Steps



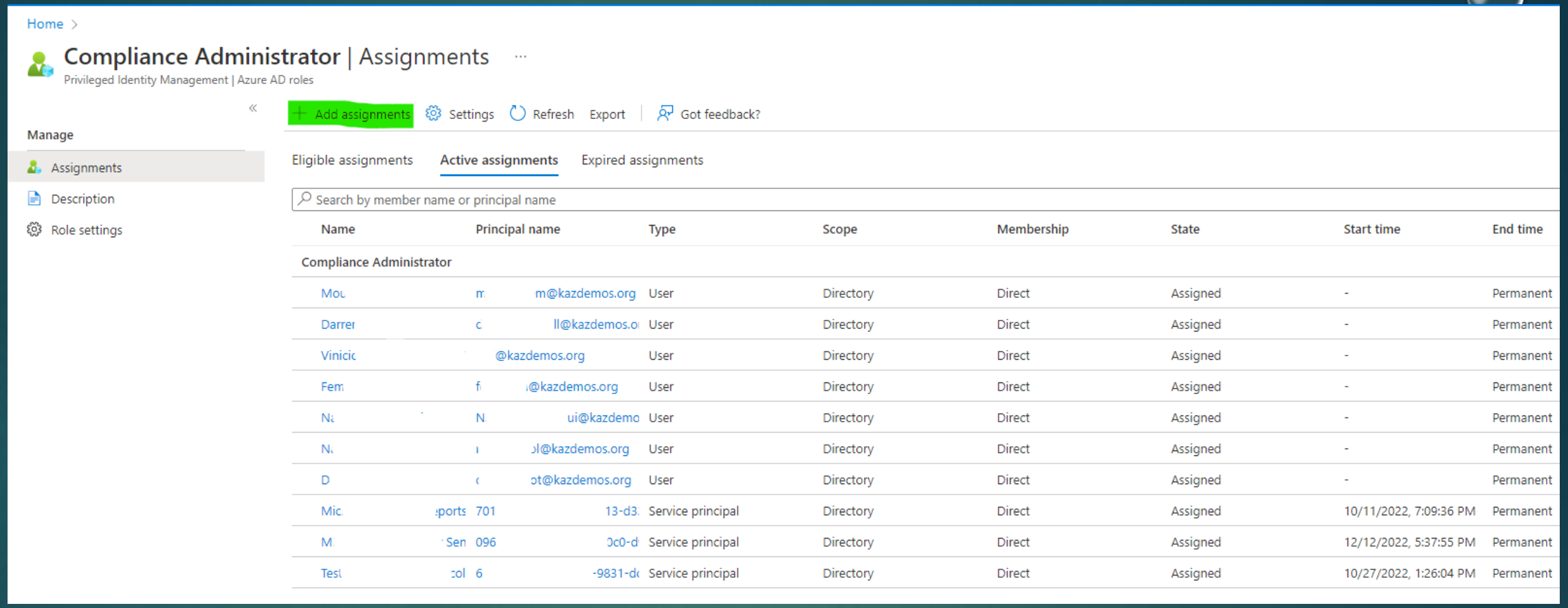
Compliance Admin Role for Script

Steps



Compliance Admin Role for Script

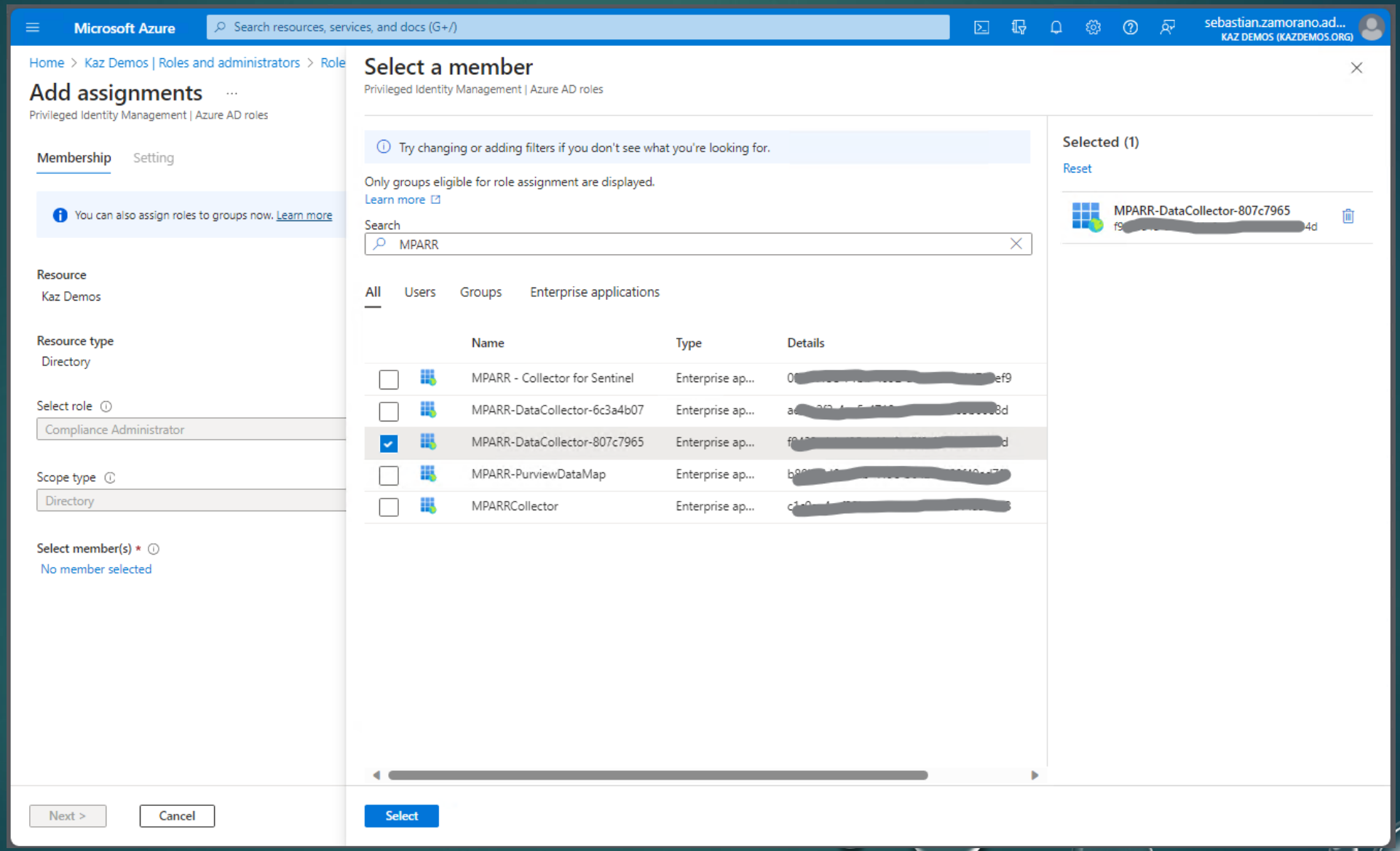
Steps



Microsoft

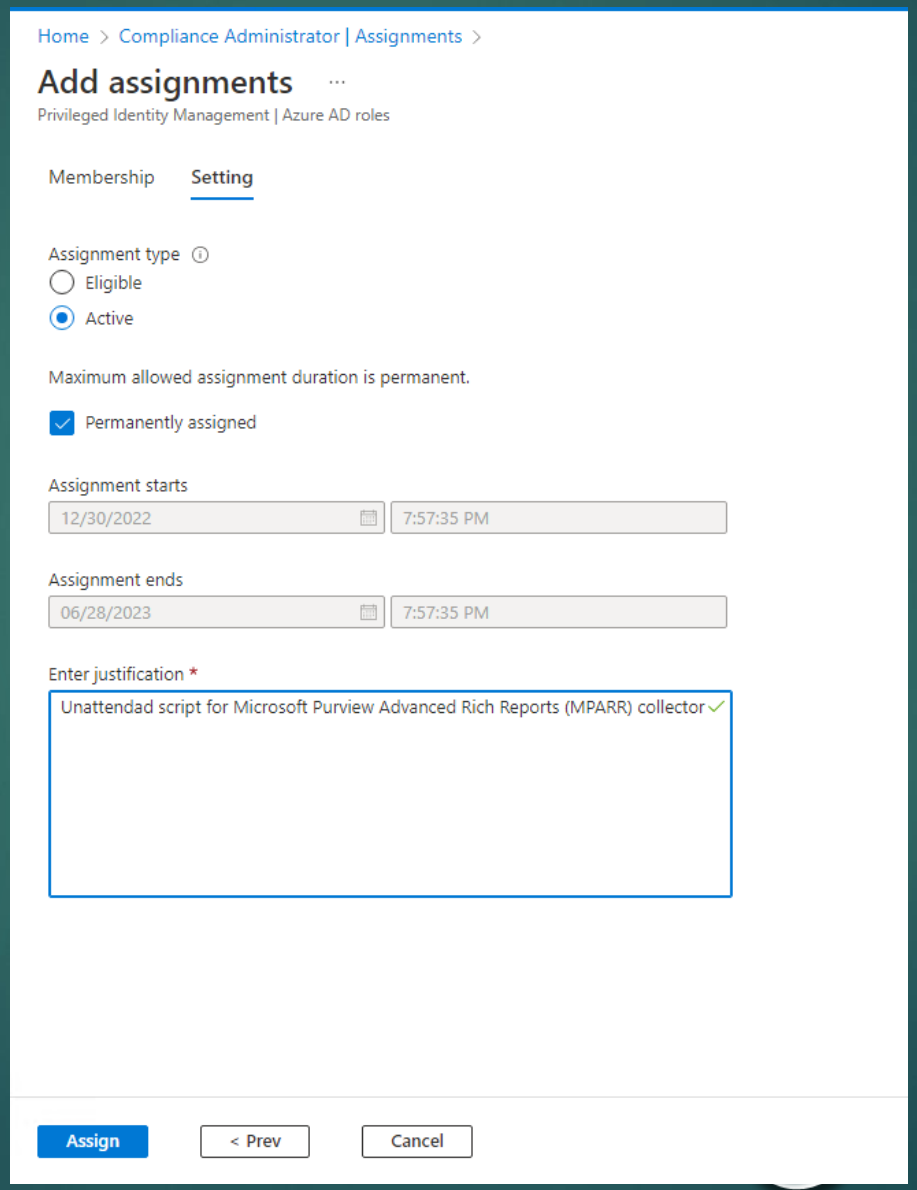
Compliance Admin Role for Script

Steps



Compliance Admin Role for Script

Steps



Microsoft

Compliance Admin Role for Script

Steps (Manual execution to avoid assign elevate privileges to Microsoft Entra App)

- In case of both scripts MPARR-LabelData.ps1 and MPARR-SITData.ps1 is the same configuration

```
154
155 Function Export-LabelData() {
156     # ---------------------------------------------------------------
157     #    Name           : Export-LabelData
158     #    Desc           : Extracts data from Get-Label into Log analytics workspace tables for reporting purposes
159     #    Return         : None
160     # ---------------------------------------------------------------
161         <#
162         .NOTES
163         If you cannot add the "Compliance Administrator" role to the Azure AD App, for security reasons, you can comment the line 167 and uncomment the line 166, in that case
164         Someone with "Compliance Administrator" role needs to execute this script, this script is executed on-demand to refresh the label names
165         #>
166         #Connect-IPPSSession
167         Connect-IPPSSession -CertificateThumbPrint $CertificateThumb -AppID $AppClientID -Organization $OnmicrosoftTenant
```

MS Purview - PowerShell

Obtain your Label list and Sensitive Information Types with IDs and send to Logs Analytics

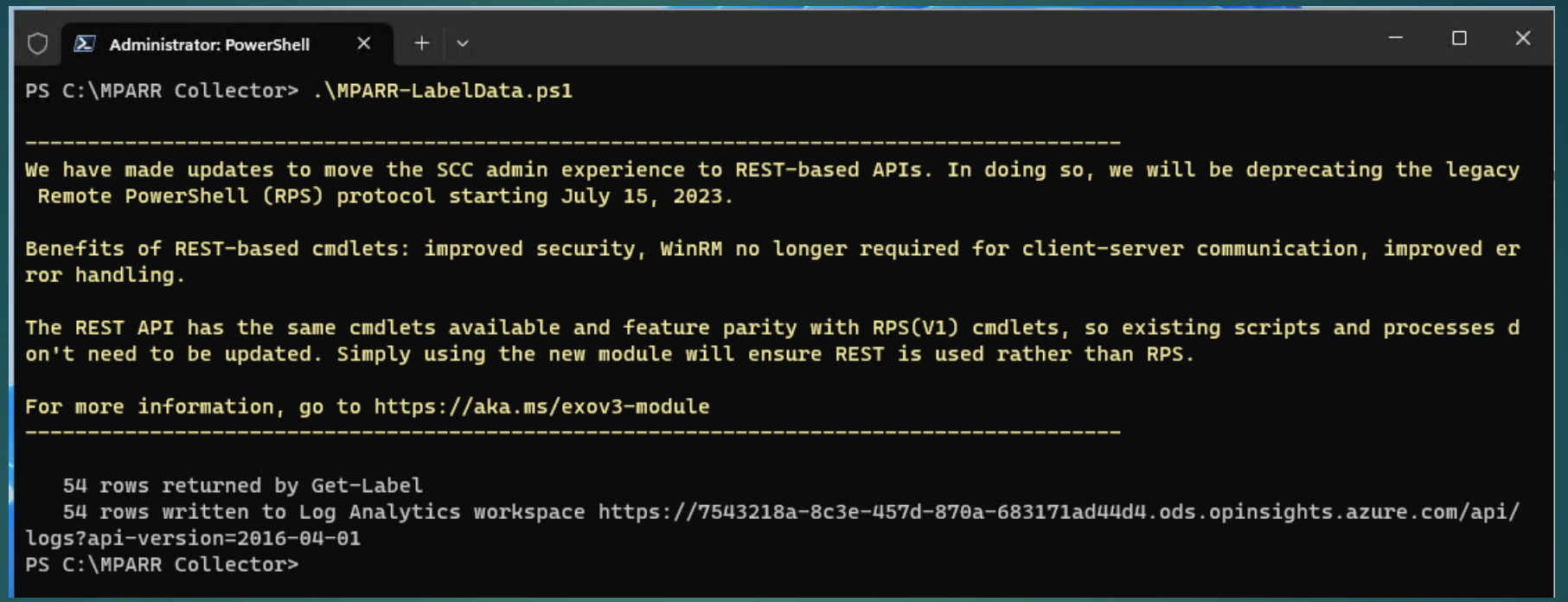
- Please complete first all this steps, **Office 365 Exchange Online API** is used to obtain the next information
- The data stored on API schemas contains only the ID of the labels, for that reason is required have a Matrix between IDs and Display Names, the script used here take the information from Information Protection Service and Import the data in Logs Analytics.
- To execute this script please complete these steps 1st.
- The script MPARR-LabelData.ps1 and MPARR-SITData.ps1 are located at the same folder where the laconfig.json file is stored, 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 validate the data in Logs Analytics, click here.
- Understanding the complexity to give elevate privileges to an unattended script, a line can be modified on both scripts to a manual execution, in this case someone with Compliance Administrator role needs to execute this script on PowerShell, this execution is on-demand and is required only when you have modified or new labels, to up to date the reports with this information, or can be required depending the retention period in the Logs Analytics workspace.

**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*

Microsoft

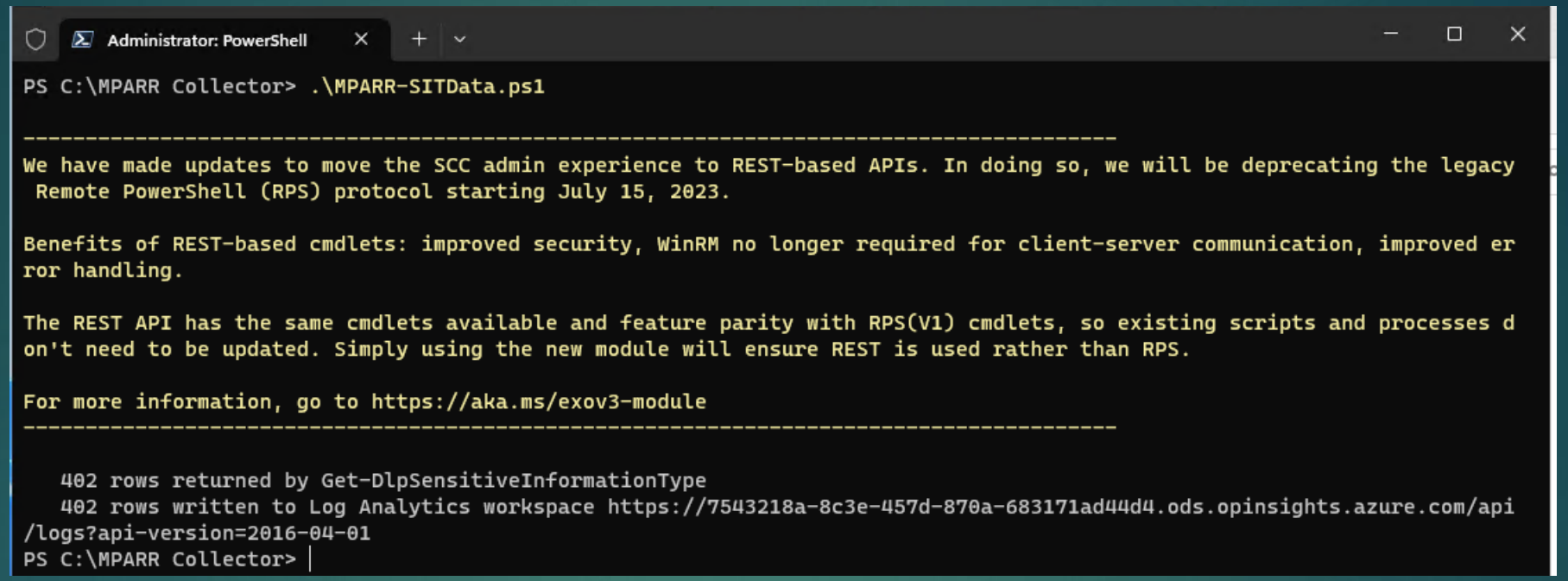
Workstation - PowerShell

STEPS



Workstation - PowerShell

STEPS



Workstation - PowerShell

STEPS

```
154
155 Function Export-LabelData() {
156     # ---------------------------------------------------------------
157     #    Name           : Export-LabelData
158     #    Desc           : Extracts data from Get-Label into Log analytics workspace tables for reporting purposes
159     #    Return         : None
160     # ---------------------------------------------------------------
161         <#
162         .NOTES
163         If you cannot add the "Compliance Administrator" role to the Azure AD App, for security reasons, you can comment the line 167 and uncomment the line 166, in that case
164         Someone with "Compliance Administrator" role needs to execute this script, this script is executed on-demand to refresh the label names
165         #>
166         #Connect-IPPSSession
167         Connect-IPPSSession -CertificateThumbPrint $CertificateThumb -AppID $AppClientID -Organization $OnmicrosoftTenant
```

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> .\MPARR-ExportCSV2LA.ps1 -FileName ".\Support\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 validate the data in Logs Analytics, 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

Microsoft

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 **MPARR-AzureADUsers.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:\MPARR Collector> .\MPARR-AzureADUsers.ps1
```

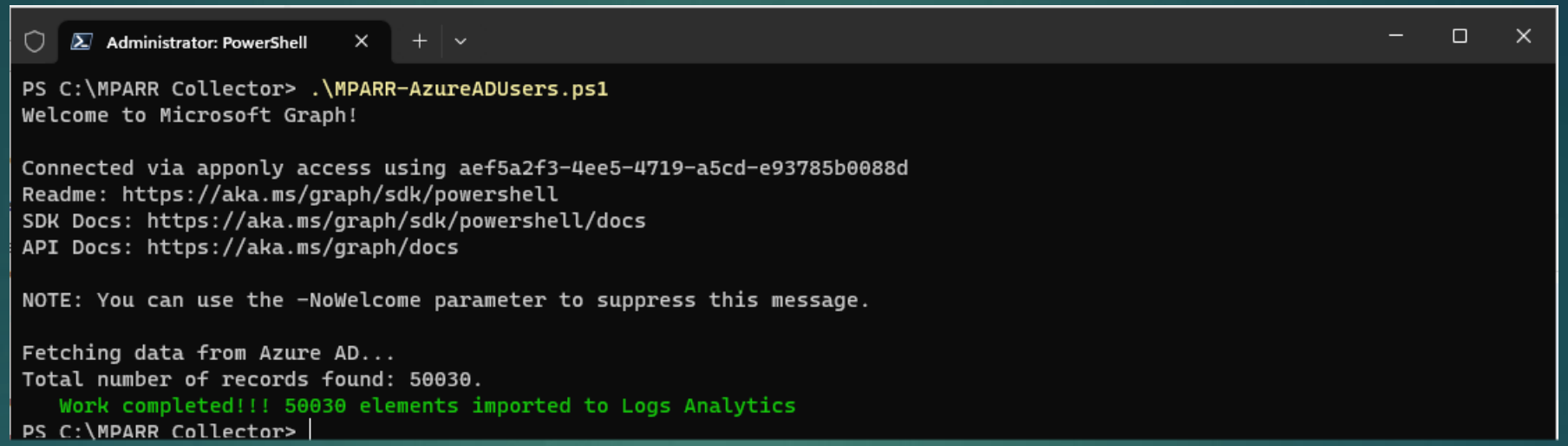
- How to validate the data in Logs Analytics, click here.

**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*

Microsoft

Powershell – Microsoft Users

STEPS



LIST OF MICROSOFT ENTRA 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 Microsoft Entra Roles, and Domains registered on the Tenant, you need execute the script **MPARR-AzureADRoles.ps1** and **MPARR-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.

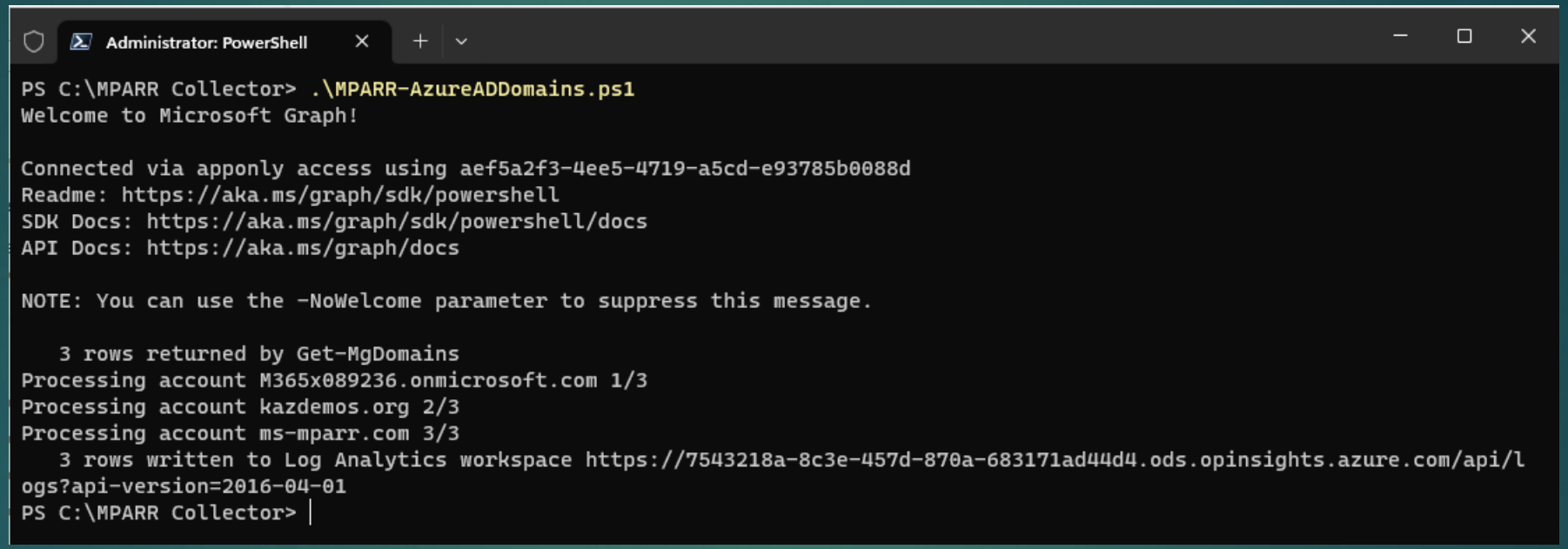
```
PS C:\Collector> .\MPARR-AzureADDomains.ps1

PS C:\Collector> .\MPARR-AzureADRoles.ps1
```

- How to validate the data in Logs Analytics, 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*

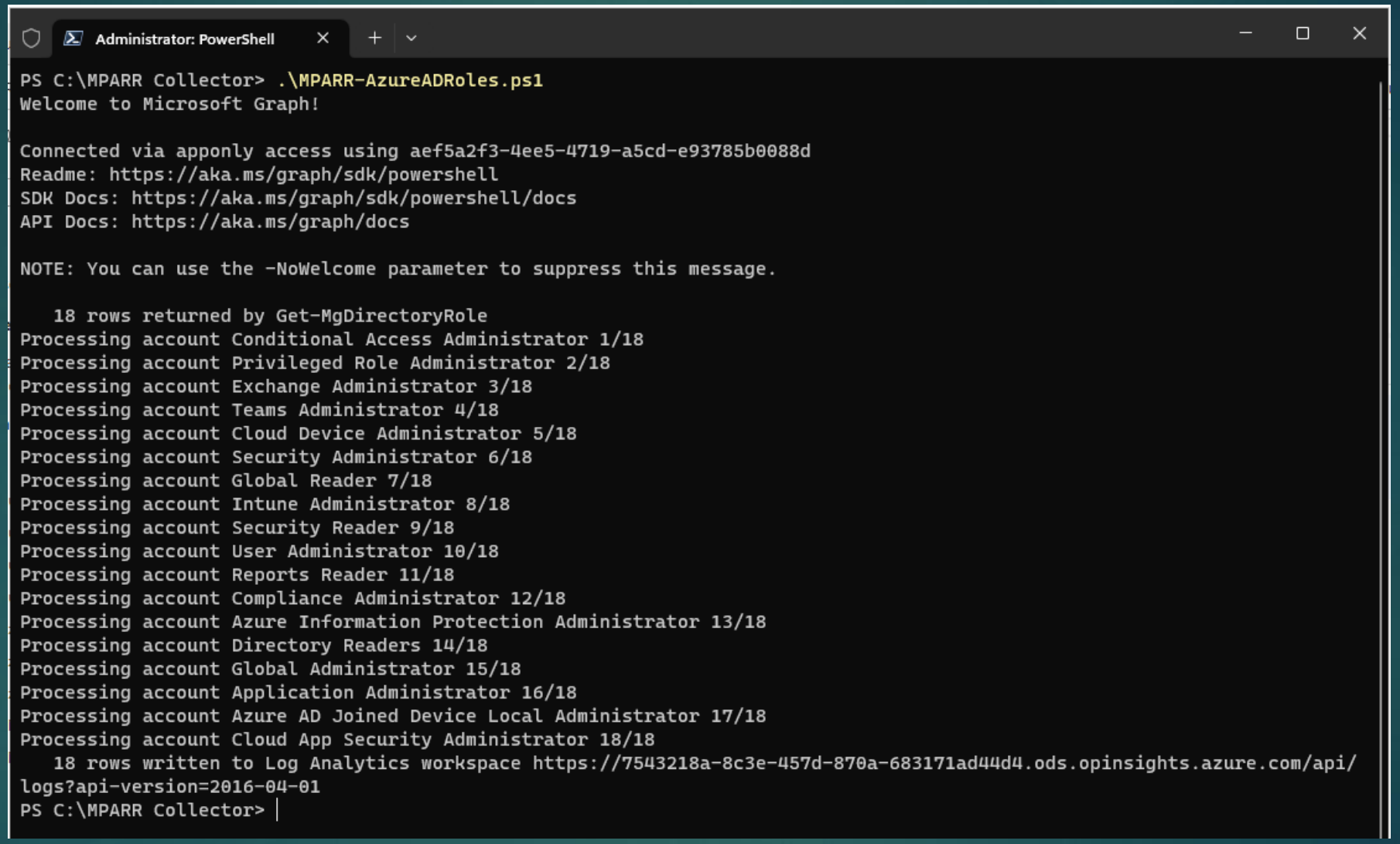
Powershell – Microsoft Entra ID

STEPS



Powershell – Microsoft Entra ID

STEPS



Microsoft

Logs Analytics workspace

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**
    - **SITs_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 any kind operation is recorded.*

Logs Analytics workspace

How to validate if we have data in our Workspace?

- On the Logs Analytics workspace under Logs menu, you can execute these KQL:
  - To check when the last hour was when data was ingested

```
<TableNameVariable_CL>
| where TimeGenerated > now(-1d)
| summarize by
    Year = datetime_part('Year',TimeGenerated),
    Month = datetime_part('Month',TimeGenerated),
    Day = datetime_part('Day',TimeGenerated),
    Hour = datetime_part('Hour',TimeGenerated)
```

  - Known about the different activities(Operations) that are collected on our workspace

```
<TableNameVariable_CL>
| where TimeGenerated > now(-1d)
| summarize count() by Operation_s
```

  - If you want to see the data recently collected, you can execute a KQL using only the name of the table, in this way:
    - Labels_CL

```
Labels_CL
```

    - MSProducts

```
MSProducts_CL
```

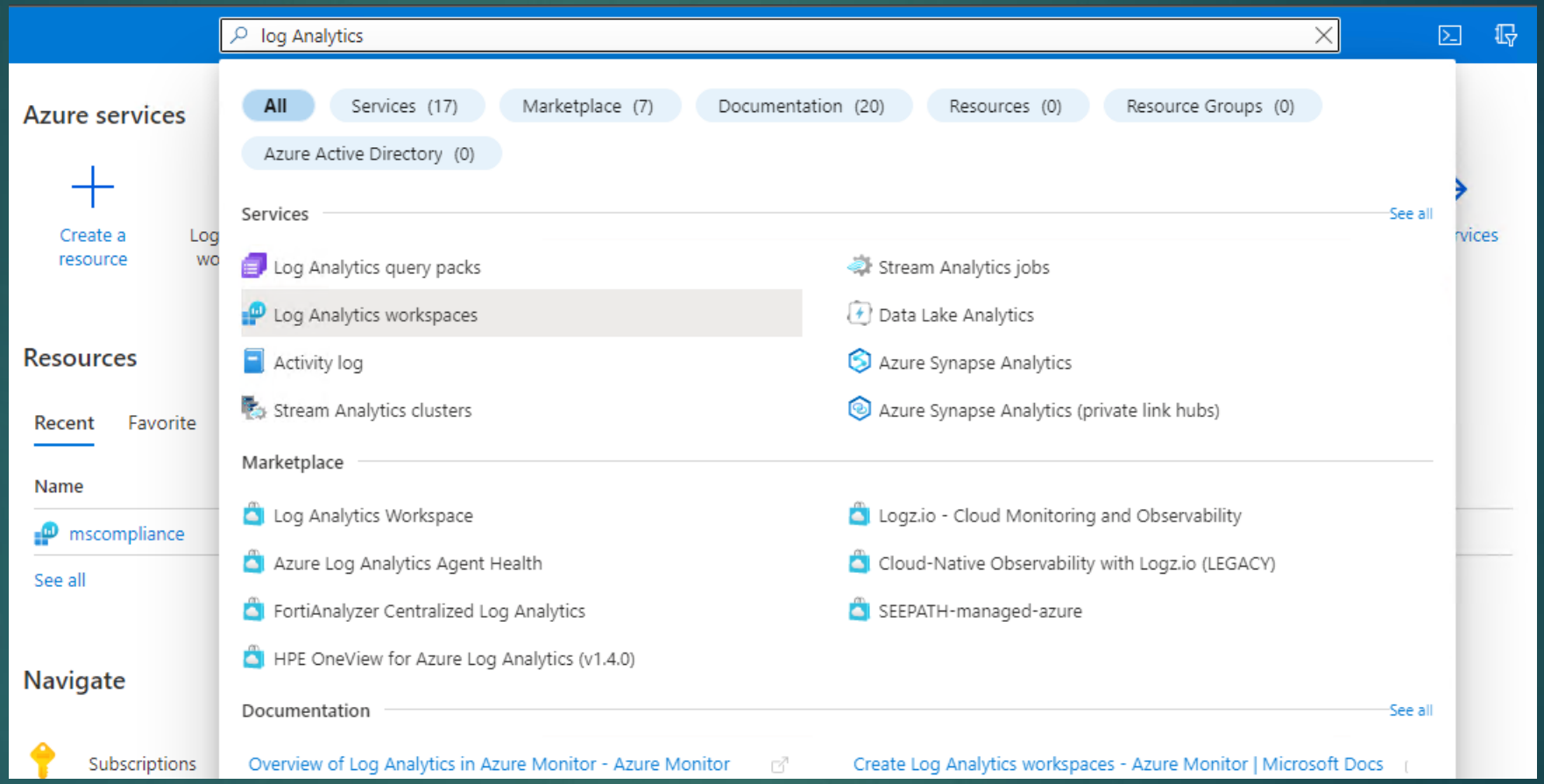
    - AzureADUsers

```
AzureADUsers_CL
```

Microsoft

Logs Analytics workspace

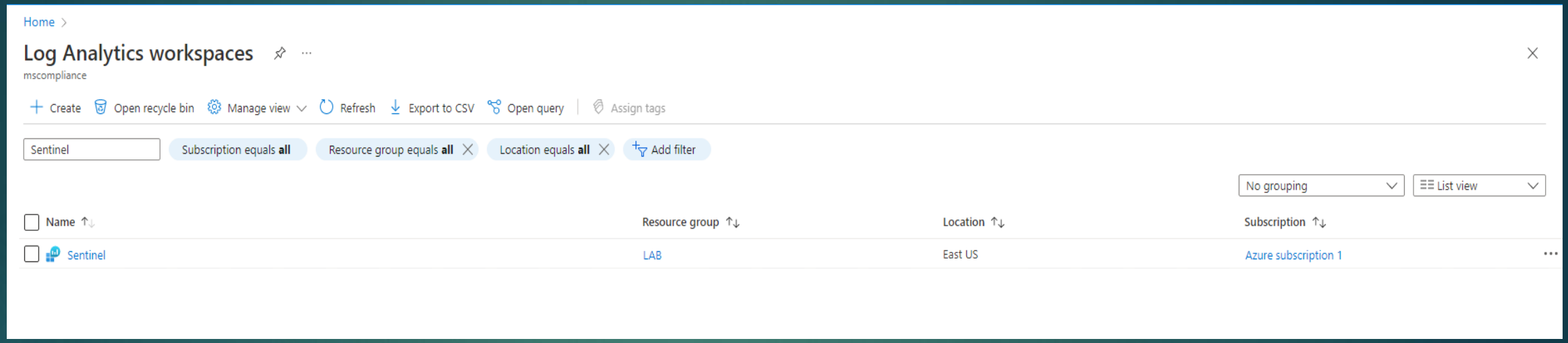
Steps



Microsoft

Logs Analytics workspace

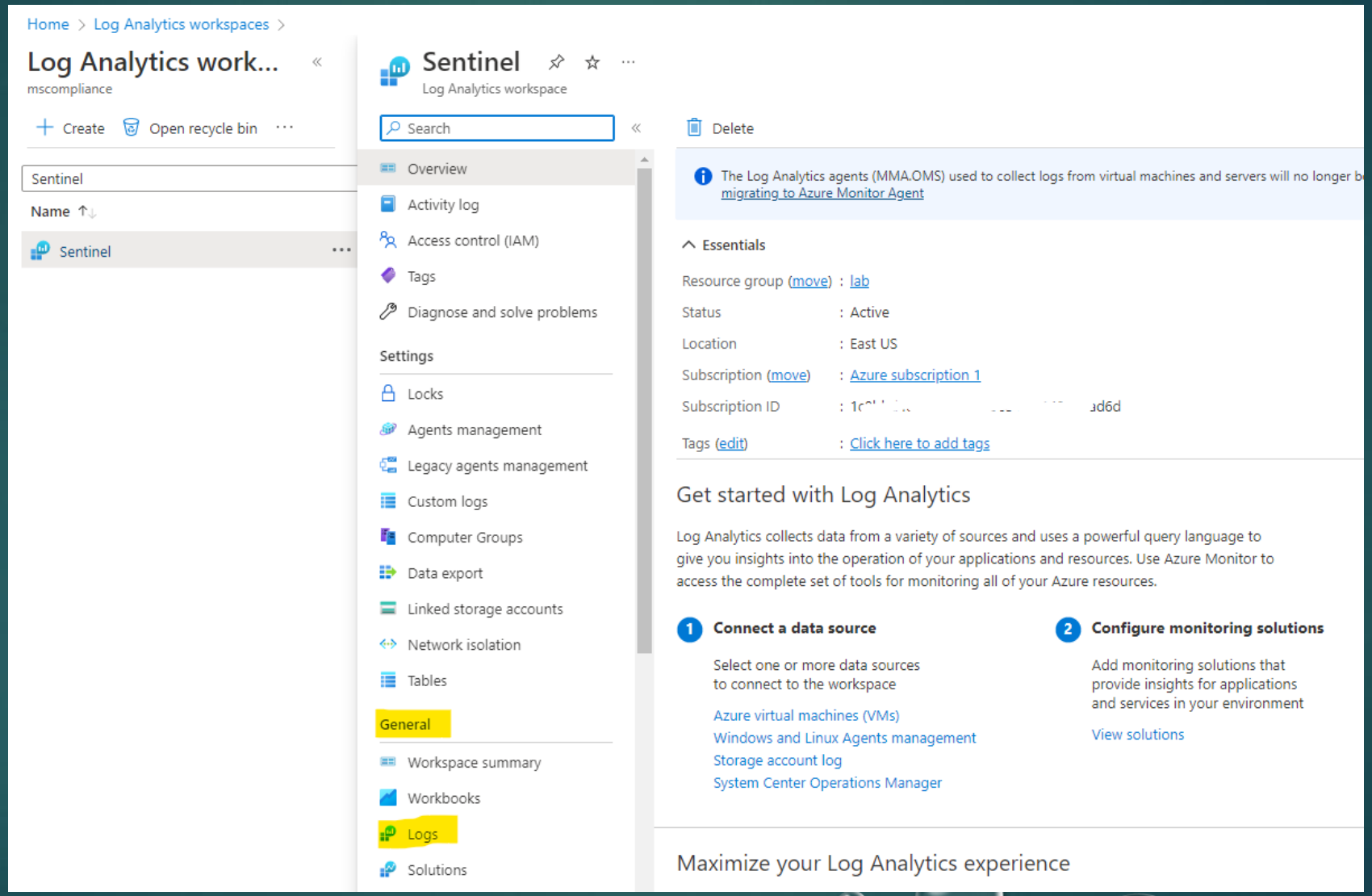
Steps



Microsoft

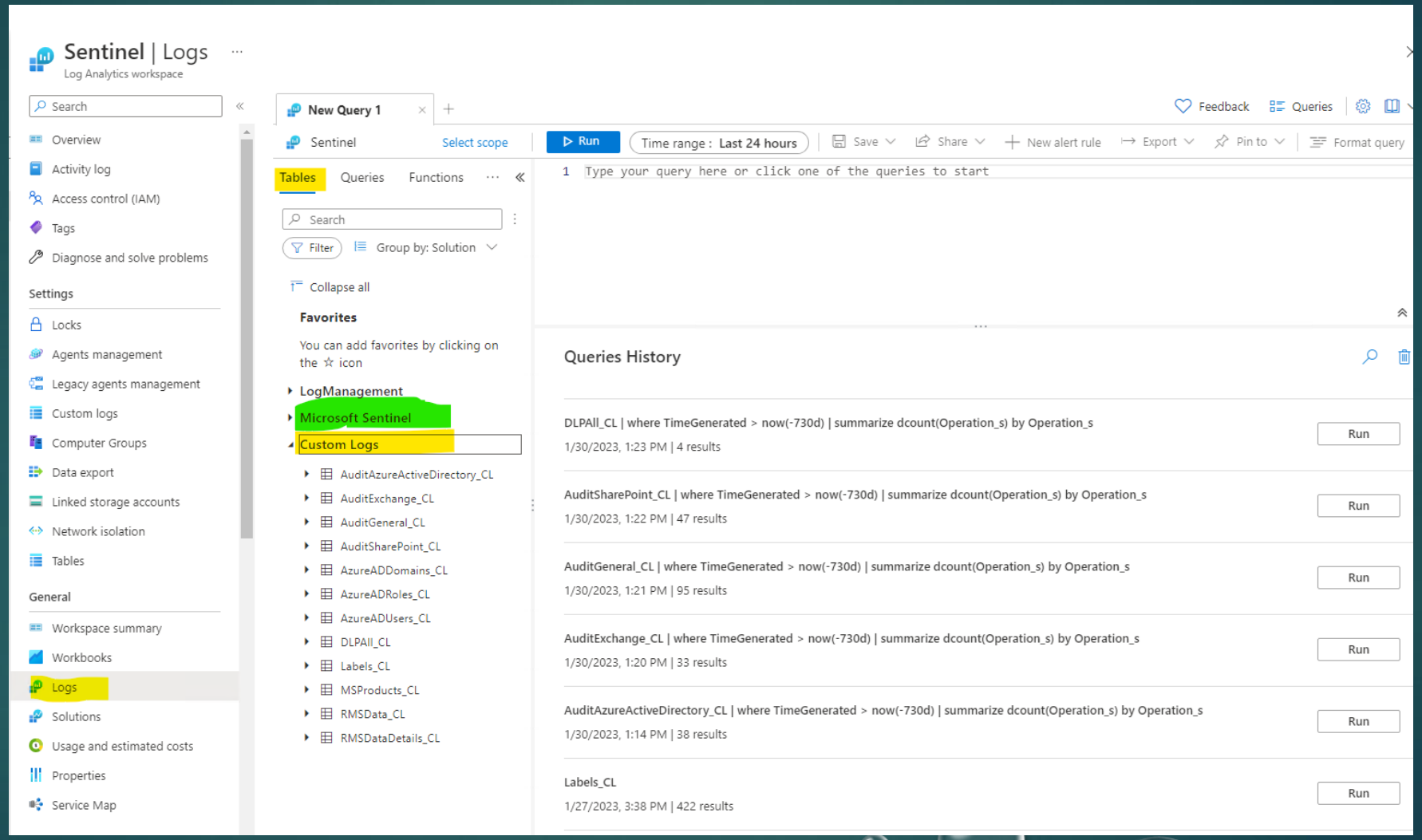
Logs Analytics workspace

Steps



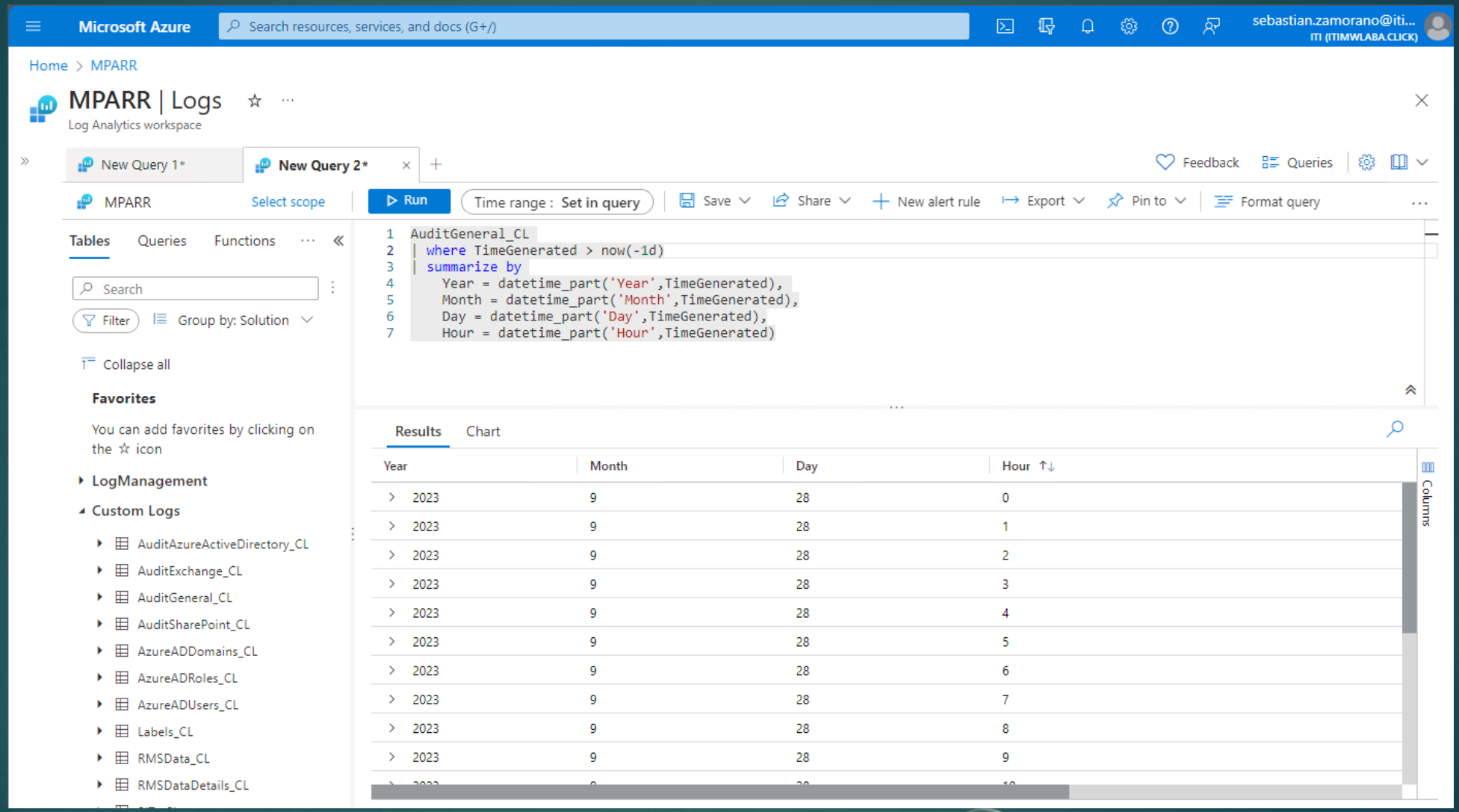
Logs Analytics workspace

Steps



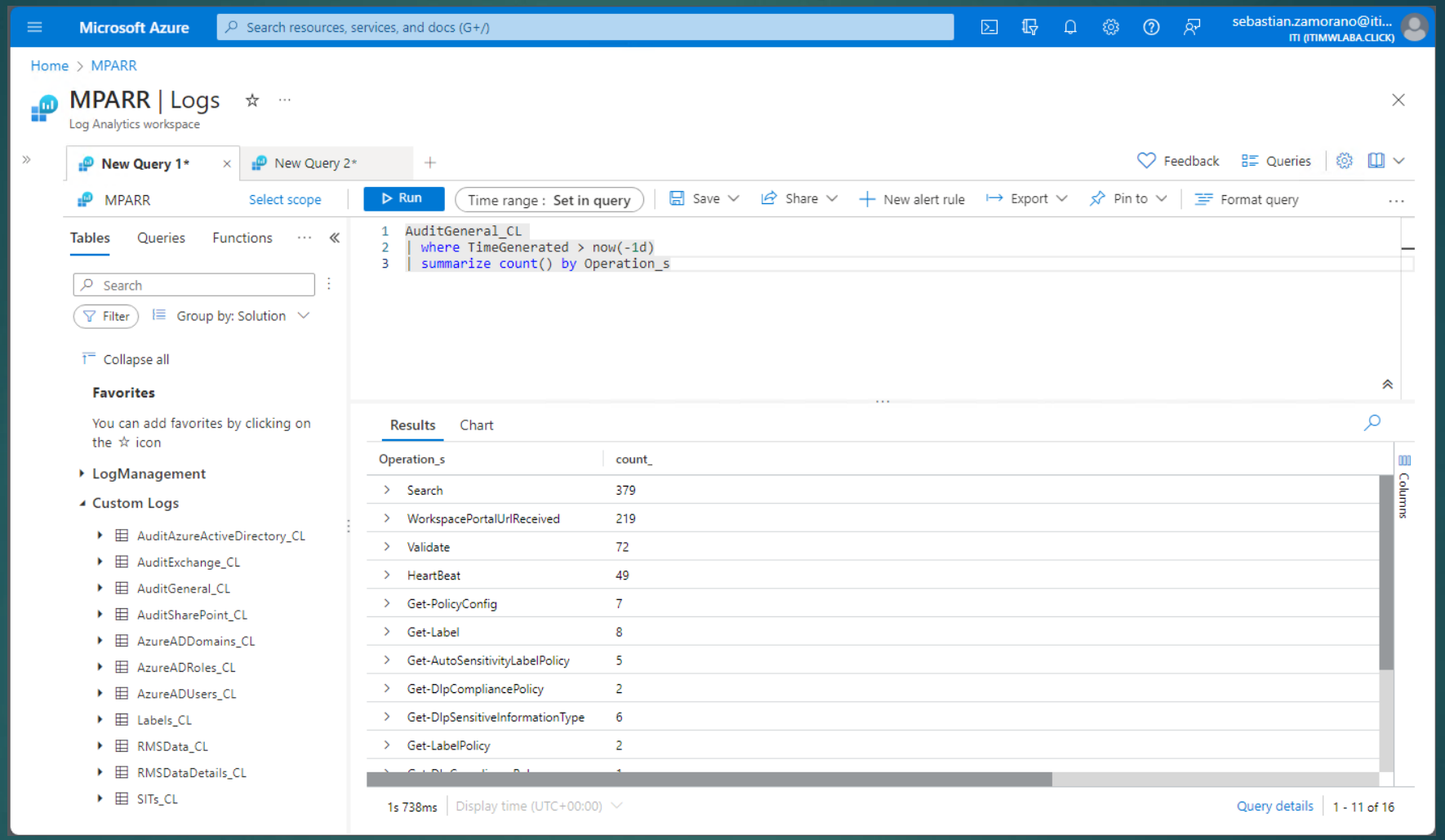
Logs Analytics workspace

Latest time where activities are log



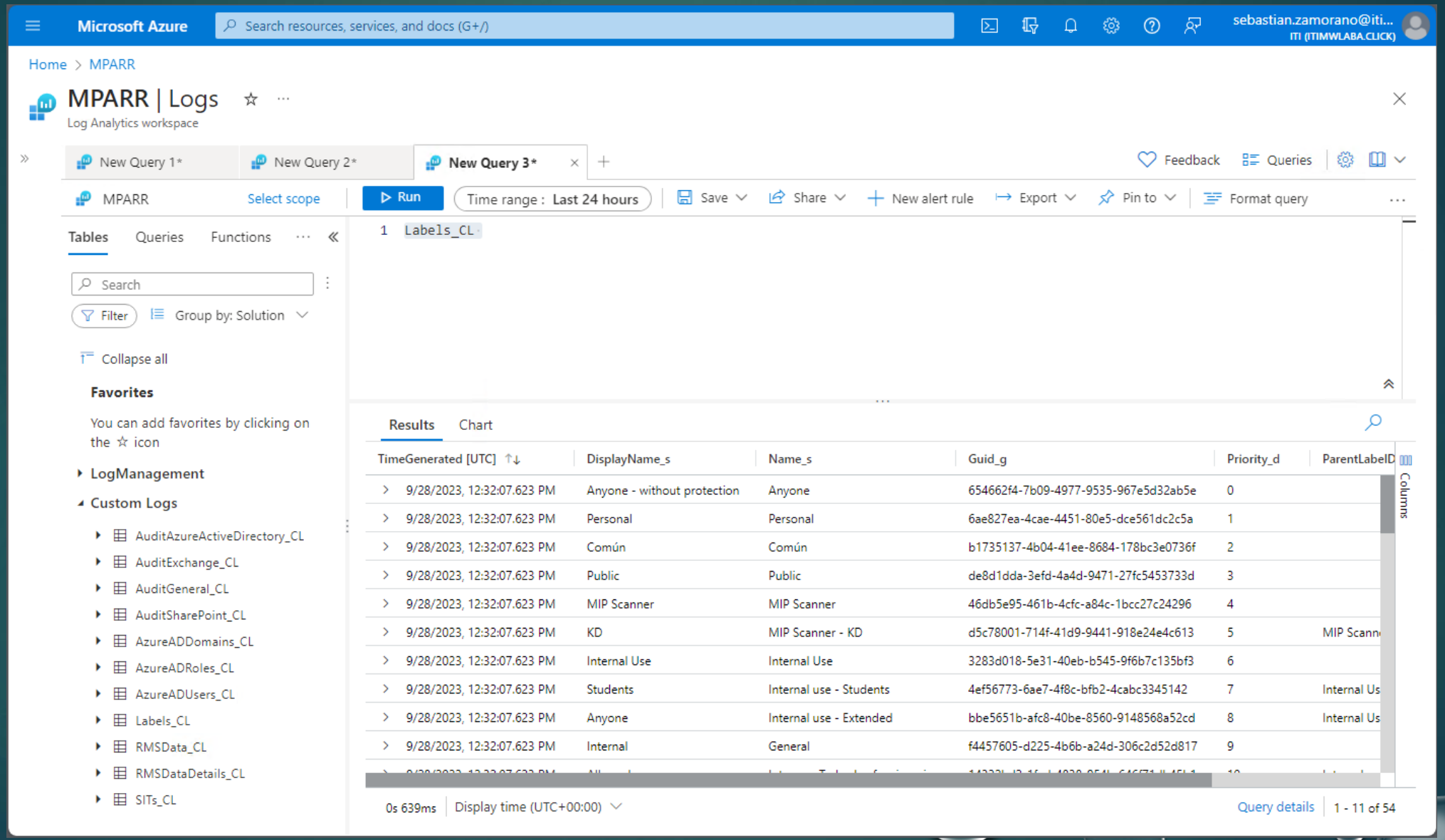
Logs Analytics workspace

Activities collect in AuditGeneral_CL in the last day



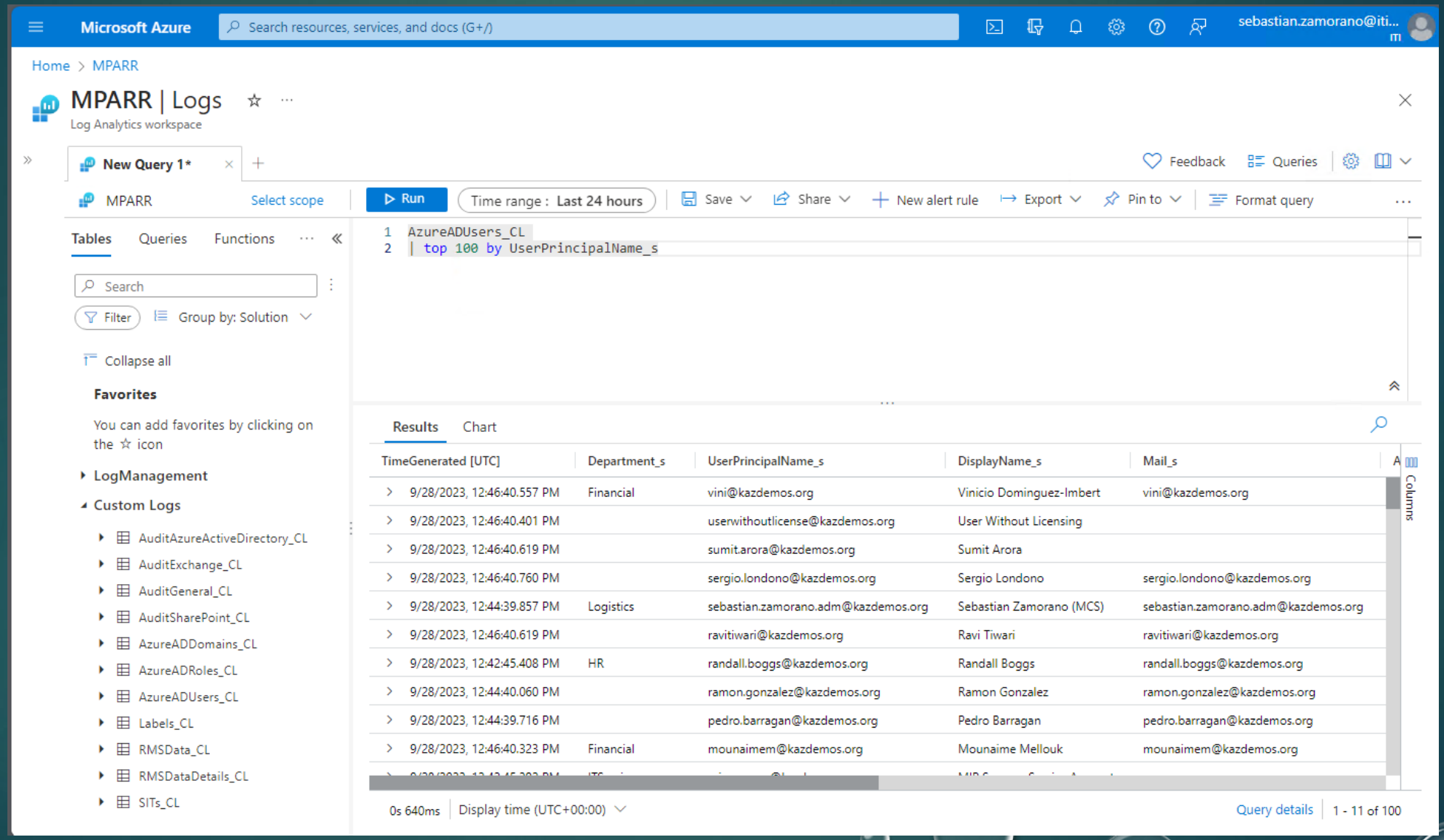
Logs Analytics workspace

Labels information



Logs Analytics workspace

Top 100 users from AzureADUsers_CL



Logs Analytics workspace

Export example

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
```

- The same can be used with other tables, only consider that the fields can be different on each case, like as:
  - AzureADUsers_CL
  - AzureADDomain_CL
  - AzureADRoles_CL
  - MSProducts_CL
  - SITs_CL

Microsoft

KQL for Latest Microsoft ENTRA 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:

```
AzureADUsers_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
```

Microsoft

Checklist to Import Power Bi Template

TO IMPORT ADVANCED POWER BI TEMPLATE

- Validate these scripts was executed first:
  - .\MPARR_Collector.ps1 and is running under task scheduler
  - .\MPARR-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)
  - .\MPARR-AzureADUsers.ps1 (run on demand)
  - .\MPARR-AzureADRoles.ps1 (run on demand)
  - .\MPARR-AzureADDomains.ps1 (run on demand)
  - .\MPARR-LabelData.ps1 (run on demand)
  - .\MPARR-SITData.ps1 (run on demand)
  - .\MPARR-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

Power BI Templates can fail if the tables doesn't exist or you try to use a template for a service that is not running in your environment, like as MIP Scanner or Endpoint DLP .

Microsoft

Power BI – Import Template

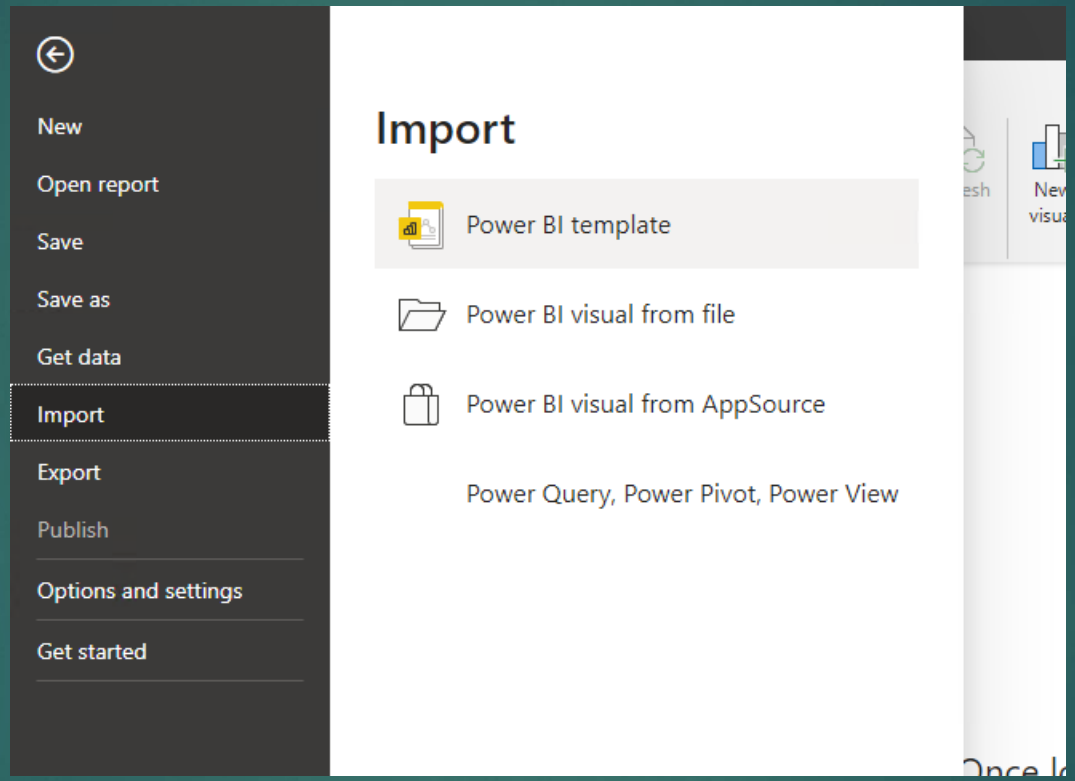
To import a Template

- 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

Microsoft

Power BI - Templates

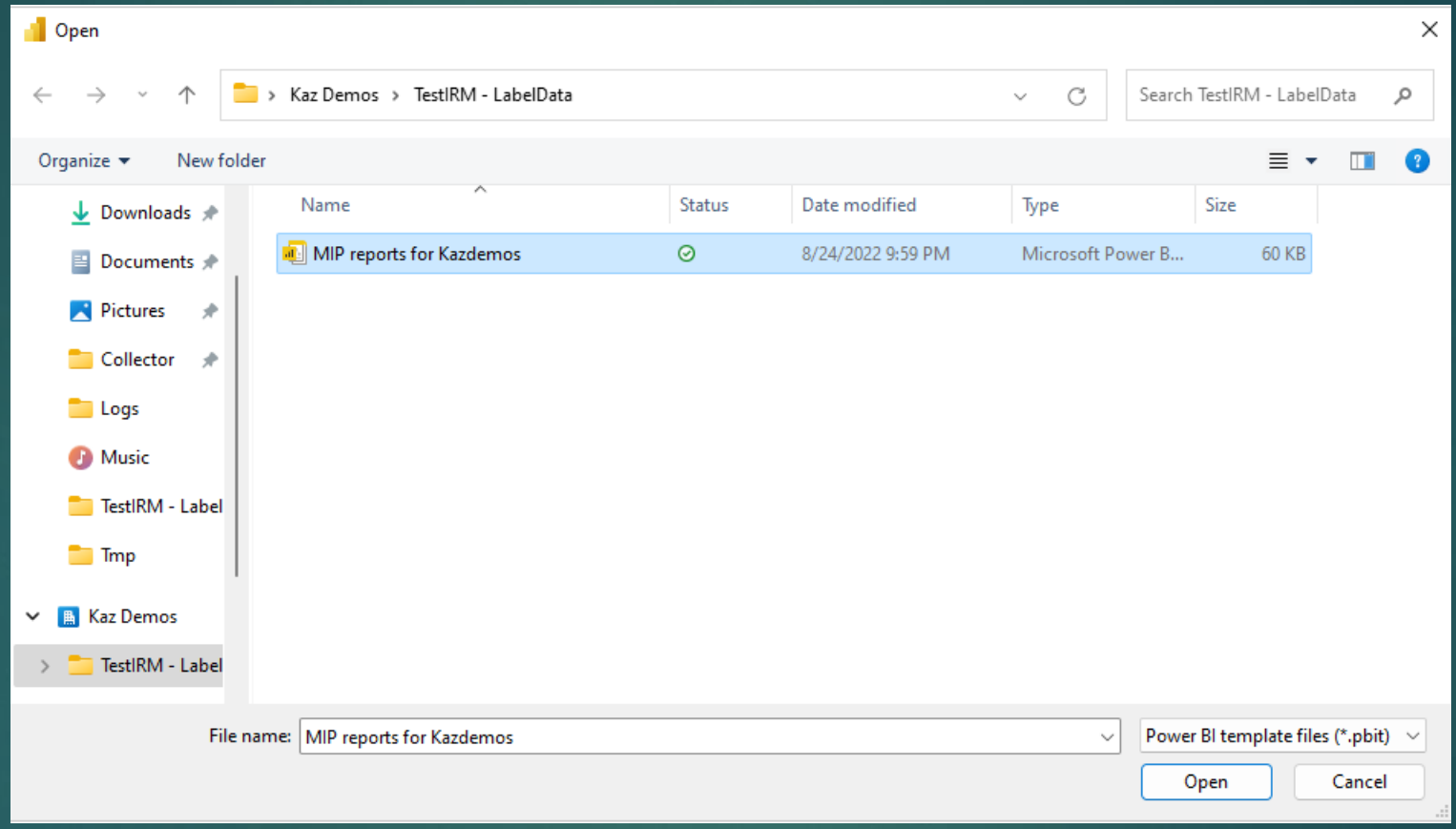
Steps



Microsoft

Power BI - Templates

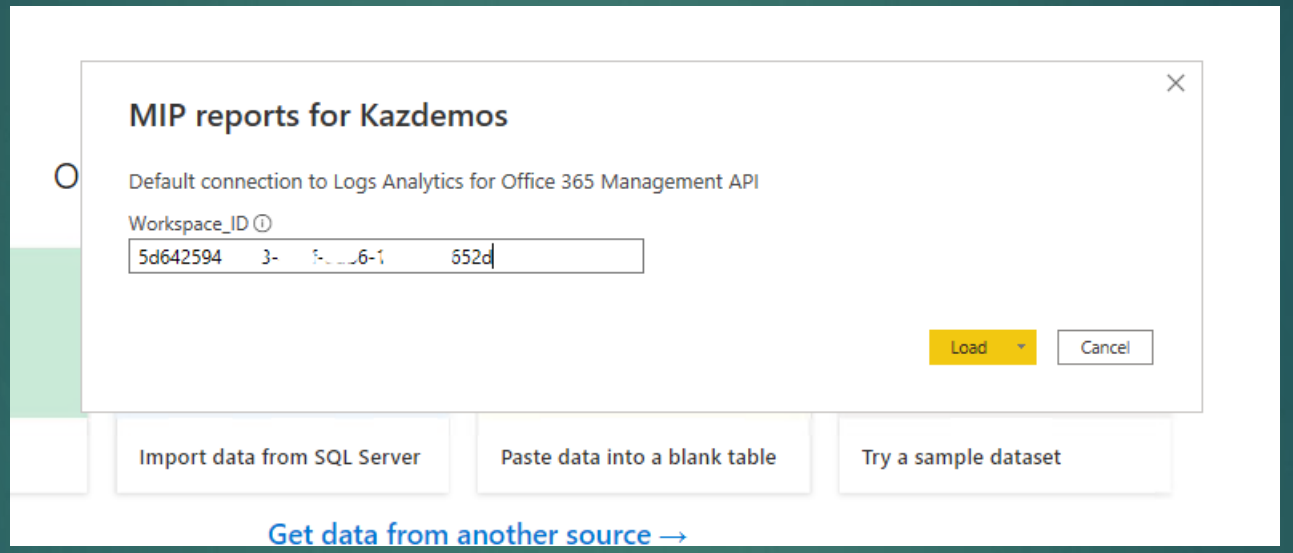
Steps



Microsoft

Power BI - Templates

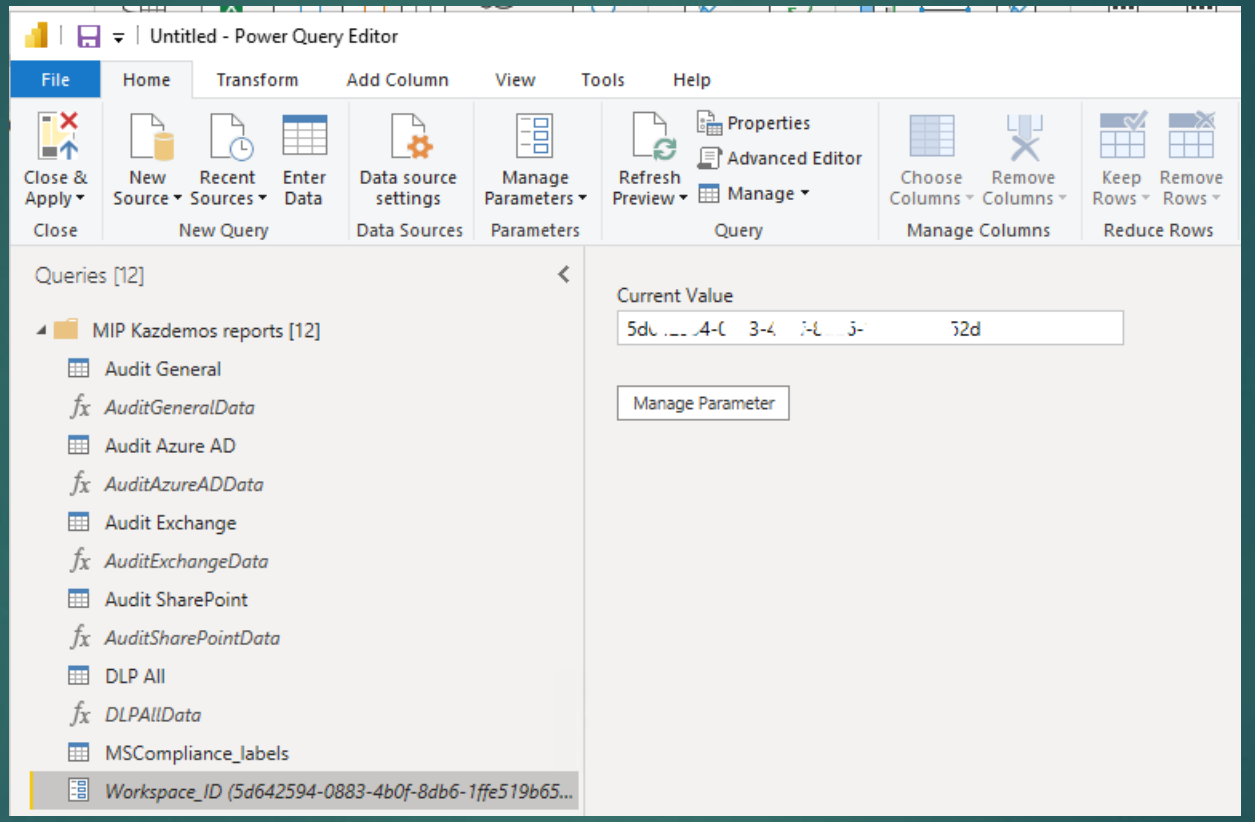
Steps



Microsoft

Power BI - Templates

Steps



Microsoft

THANK YOU

Sebastián Zamorano

+56 9 5207 3058

sebastian.zamorano@microsoft.com

https://aka.ms/MPARR-GitHub

https://aka.ms/MPARR-LinkedIn

https://aka.ms/MPARR-YouTube

Microsoft