

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



DASHBOARDS

SOME SAMPLE REPORTS

Dashboard - Overview

Dashboard for Unified Labeling behavior

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

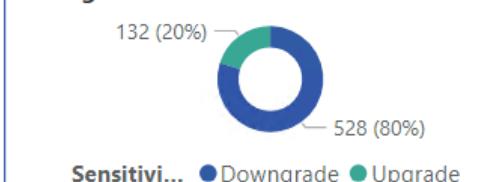
Number of files by Has Label



Number of user owned files by Has Label



Number of label changes by Sensitivity Change



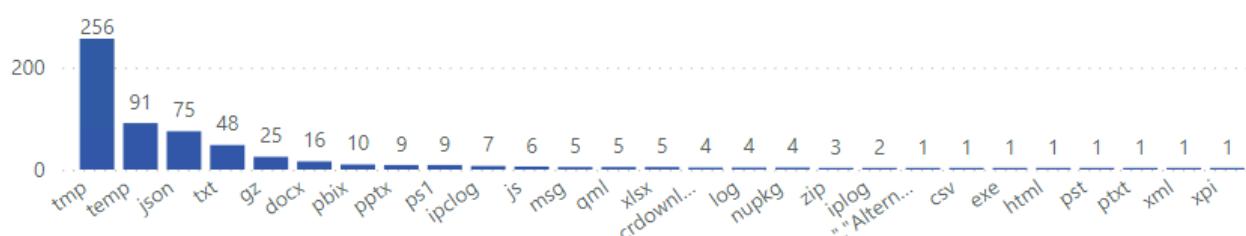
Labeled files by label name



Number of user owned files by WebService and Has Label



File count by extension



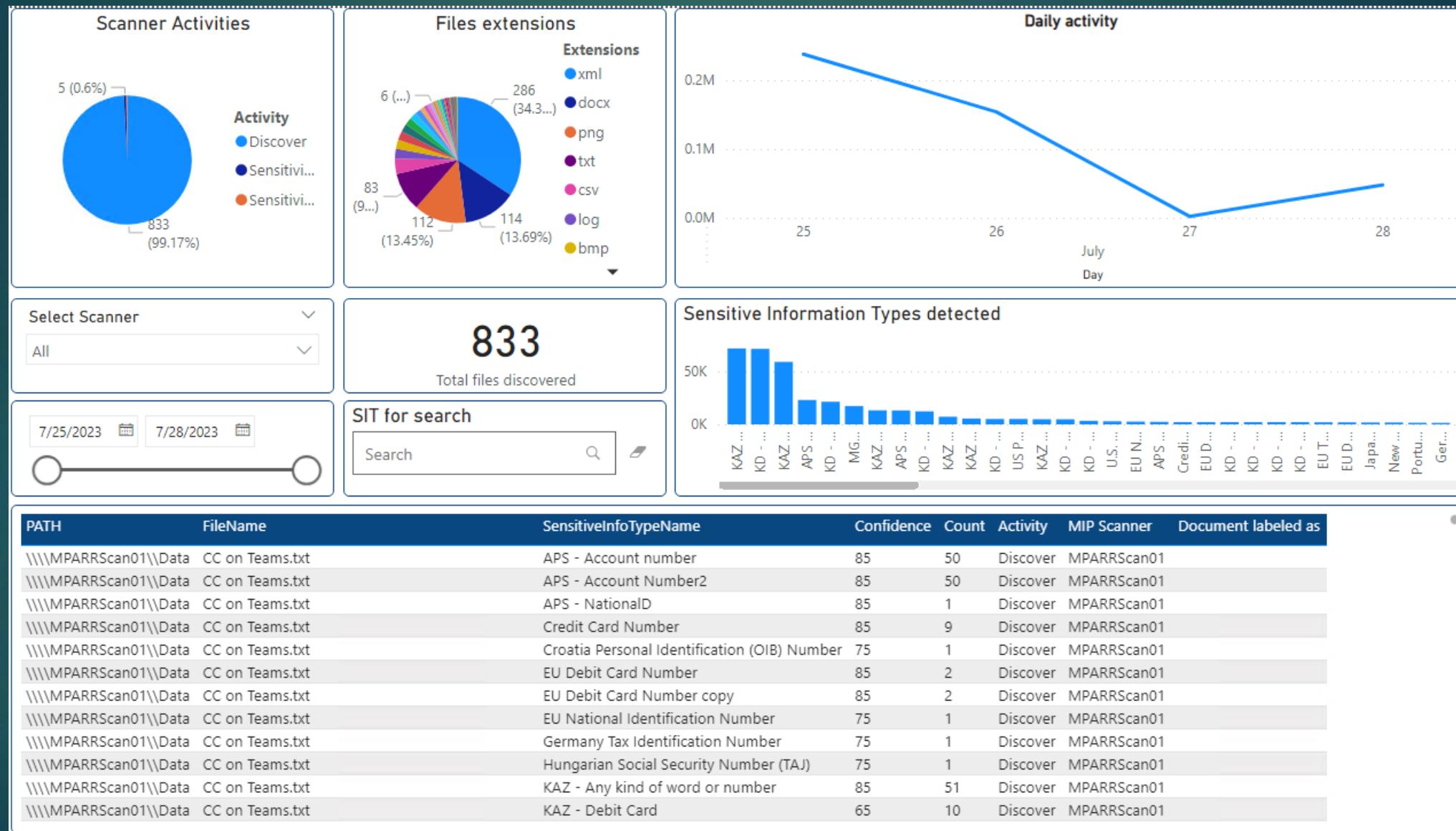
User

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



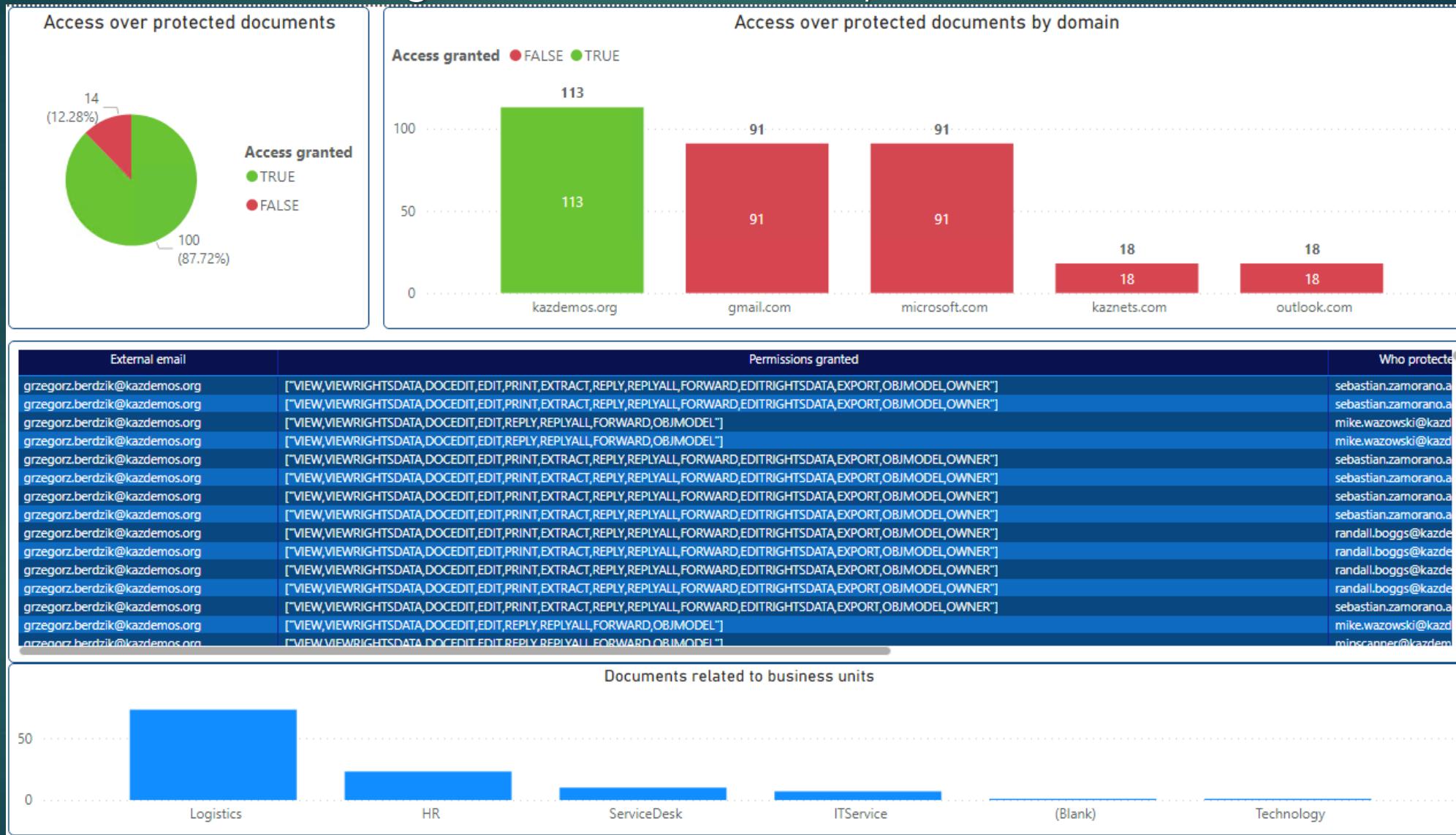
Dashboard – MIP Scanner

Dashboard for MIP Scanner activities



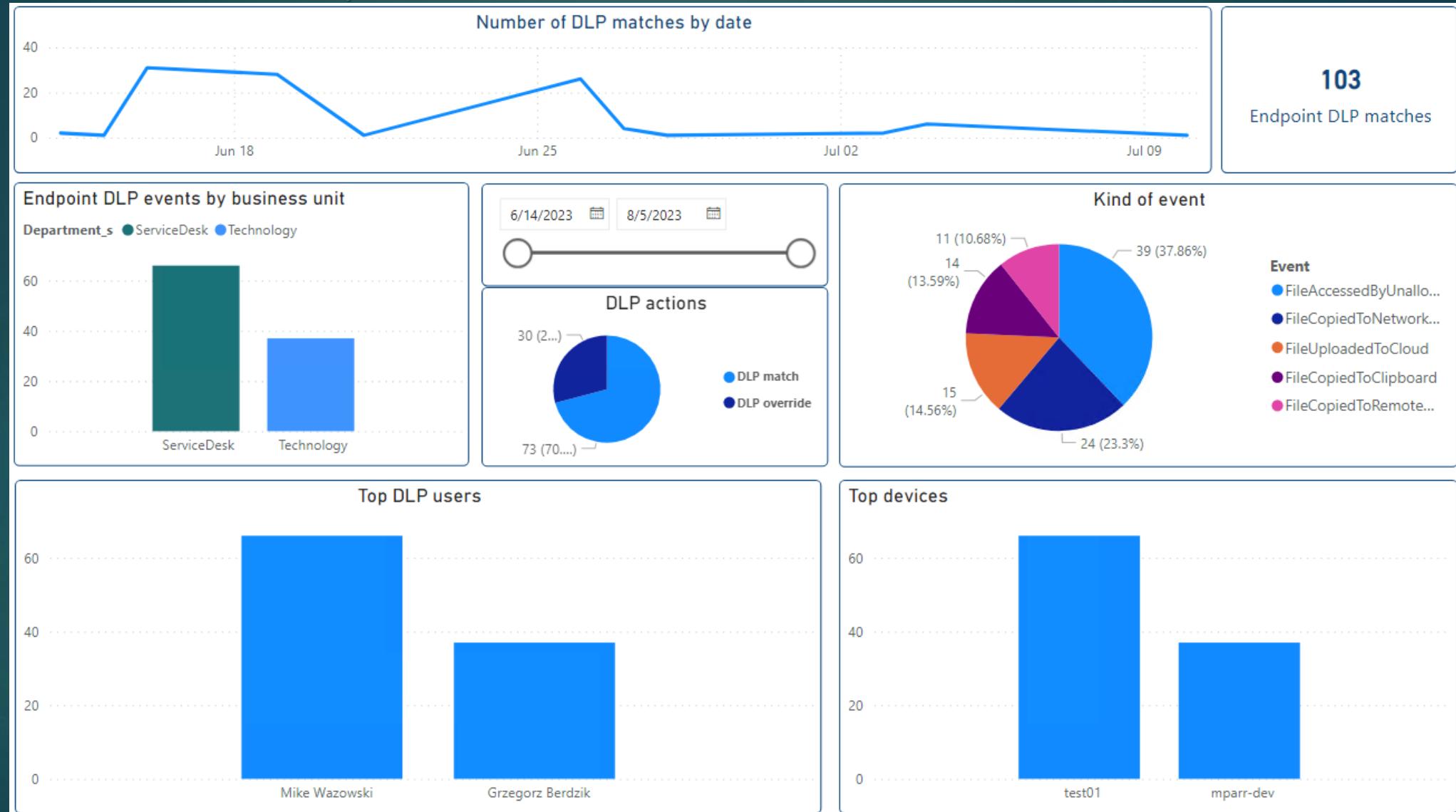
Dashboard – RMS Protection

Dashboard for access granted and denied for protected documents



Dashboard – Endpoint DLP

Dashboard for endpoint DLP activities



Dashboard - DLP Details

Dashboard for SPO DLP detailed activities

Number of DLP matches by date

Date	Matches
June 20	~10
June 21	~10
June 23	~10
June 27	~10
July 1	~10
July 3	~10
July 17	~10
July 23	~10
July 24	~180
July 25	~10
July 26	~10
July 27	~10
July 28	~10
July 29	~10

252
Rules matches

M365 Service
SIT name
User
File name
6/20/2023
7/29/2023

All
credit
Search
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_Plls.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

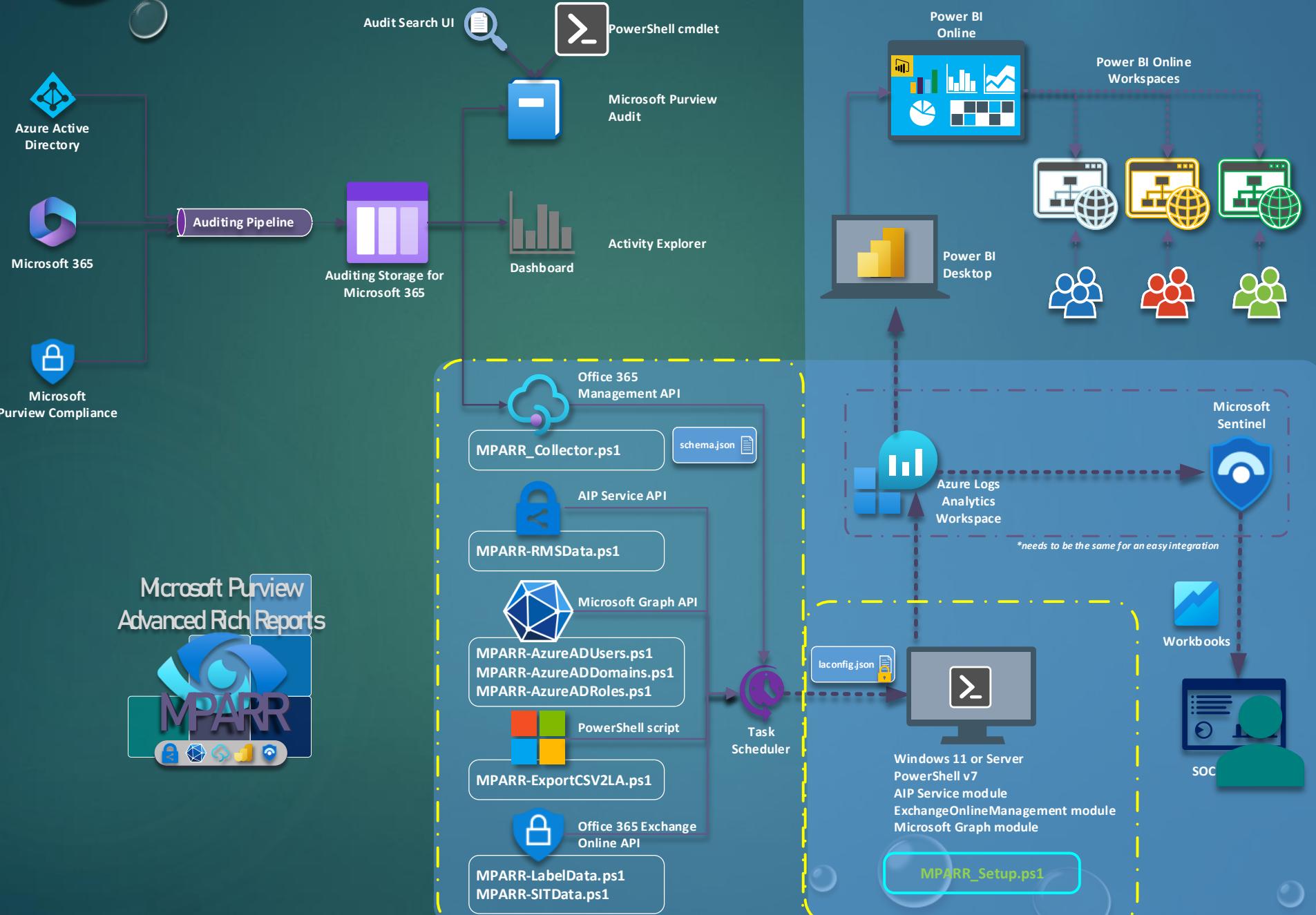
MPARR
[Kaz demos](#)

SOME STUFFS TO TAKE ON MIND

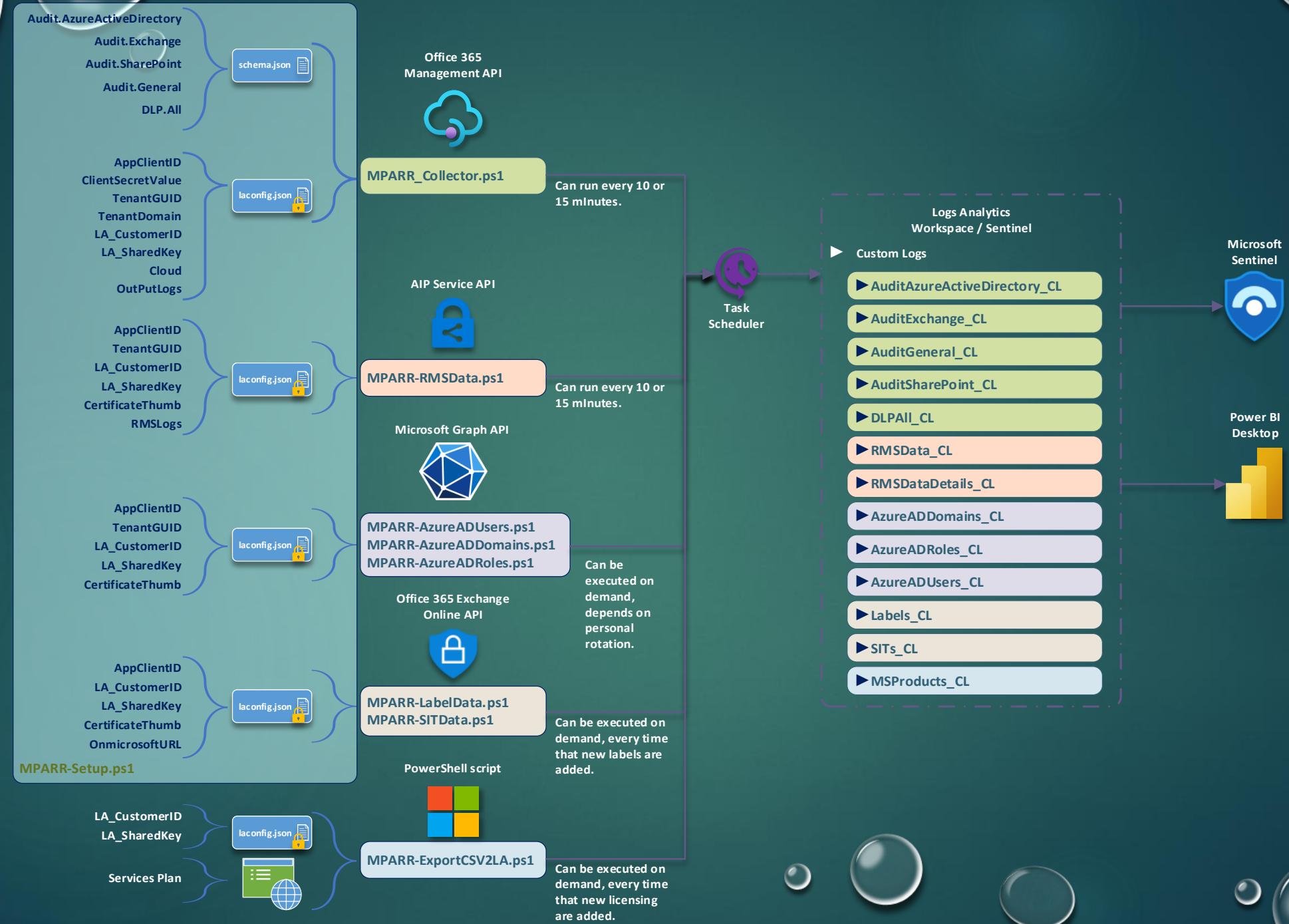


Capabilities to implement previously reports shown depends to implement MPARR as your solution to collect all the information available through Office 365 Management API, and supporting APIs, if some of the scripts are not implemented, the reports can be not implemented in the right way.

MPARR Architecture



Detailed Architecture



Detailed Architecture



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 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>

GO DIRECTLY FROM HERE TO THE SPECIFIC TOPICS

- Workspace Logs Analytics configuration →
- Download MPARR →
- Install MPARR →
- Final steps to configure MPARR →
- Additional permissions can be required →
- MPARR to collect Display Names and IDs for Labels and SITs →
- MPARR to identify Friendly licensing names →
- MPARR to collect Microsoft Entra ID(previously called Azure AD) attributes →
- Logs Analytics workspace consumption →
- Some tips →
- Next step user a Power BI Template→

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.



Logs Analytics workspace

Steps

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

- Services:**
 - Log Analytics query packs
 - Log Analytics workspaces (highlighted)
 - Activity log
 - Stream Analytics clusters
- Marketplace:**
 - Log Analytics Workspace
 - Azure Log Analytics Agent Health
 - FortiAnalyzer Centralized Log Analytics
 - HPE OneView for Azure Log Analytics (v1.4.0)
 - Logz.io - Cloud Monitoring and Observability
 - Cloud-Native Observability with Logz.io (LEGACY)
 - SEEPATH-managed-azure
- Documentation:**
 - Overview of Log Analytics in Azure Monitor - Azure Monitor
 - Create Log Analytics workspaces - Azure Monitor | Microsoft Docs



Logs Analytics workspace

Steps

The screenshot shows the Microsoft Azure Log Analytics workspaces interface. At the top, there is a navigation bar with the title "Microsoft Azure (Preview)" and a search bar labeled "Search resources, services, and docs (G+/-)". Below the navigation bar, the page title is "Log Analytics workspaces" with a "Home >" link. There are several action buttons: "+ Create", "Open recycle bin", "Manage view", "Refresh", "Export to CSV", "Open query", and "Assign tags". Below these buttons are filter options: "Filter for any field...", "Subscription equals 3 of 48 selected", "Resource group equals all", "Location equals all", and "Add filter". The main table area has columns for "Name" (with an up-down sort arrow), "Resource group" (with an up-down sort arrow), and "Location" (with an up-down sort arrow). The "Name" column contains a single entry: "Logs Analytics workspace".



Logs Analytics workspace

Steps

Home > Log Analytics workspaces >

Create Log Analytics workspace

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) X

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

Project details

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

Subscription * ⓘ Microsoft Azure Internal Consumption (Preview) ...

Resource group * ⓘ kazdemos.org ▼
[Create new](#)

Instance details

Name * ⓘ M365Reports ✓

Region * ⓘ Central US ▼

[Review + Create](#) [« Previous](#) [Next : Tags >](#)



Logs Analytics workspace

Steps

The screenshot shows the Microsoft Azure (Preview) interface with the title "Microsoft.LogAnalyticsOMS | Overview". The left sidebar includes links for Home, Overview (which is selected), Inputs, Outputs, and Template. The main content area displays a message: "We'd love your feedback! →". Below it, a green checkmark icon indicates "Your deployment is complete". Deployment details are listed: Deployment name: Microsoft.LogAnalyticsOMS, Subscription: Microsoft Azure Internal Consumption (8c9c38d5-57e...), Resource group: kazdemos.org, Start time: 19/8/2022, 16:59:35, Correlation ID: fe71f61b-0d3f-4eeb-8ce6-3615b0384a1f. A "Go to resource" button is at the bottom.

Microsoft Azure (Preview)

Search resources, services, and docs (G+/)

Home >

Microsoft.LogAnalyticsOMS | Overview

Deployment

Search (Ctrl+ /) <>

Delete Cancel Redeploy Download Refresh

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.LogAnalyticsOMS
Subscription: Microsoft Azure Internal Consumption (8c9c38d5-57e...)
Resource group: kazdemos.org

Start time: 19/8/2022, 16:59:35
Correlation ID: fe71f61b-0d3f-4eeb-8ce6-3615b0384a1f

Deployment details

Next steps

Go to resource



Extend your data retention until 2 years

Under General select Usage and estimated costs and then Data Retention, set Data Retention period.

MCAR-Kazdemos | Usage and estimated costs

Log Analytics workspace

Search (Ctrl+ /) Usage details Insights Daily cap Data Retention Help

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

Pricing Tiers

Pay-as-you-go Recommended Tier Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about Log Analytics pricing.

Estimated costs

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

This is the current pricing tier.

Data Retention

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

Data Retention (Days) 730

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

OK

Billable data ingestion per solution (last 90 days)

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

Data ingested per solution (last 90 days)

Category

No data

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.

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

The screenshot shows a GitHub repository page for the MPARR Collector. The repository is owned by Microsoft and is a public template. The main navigation bar includes links for Product, Solutions, Open Source, Pricing, Search or jump to..., Sign in, and Sign up.

The repository name is `microsoft / Microsoft-Purview-Advanced-Rich-Reports-MPARR-Collector`. The repository has 1 issue, 48 commits, 6 forks, and 37 stars. The `Code` tab is selected, showing the main branch with 1 branch and 0 tags. The commit history lists several files and their changes:

- Installation Guide (Create MPARR- Installation Guide - Mar23.zip)
- MPARR Collector (New Get-SITData script added)
- Support Information (Create Templates.zip)
- .gitignore (Initial commit)
- CODE_OF_CONDUCT.md (CODE_OF_CONDUCT.md committed)
- DLP-Reports-Samples.md (Update DLP-Reports-Samples.md)
- LICENSE (LICENSE committed)
- MPARR Collector.zip (New Get-SITData script added)
- README.md (Update README.md)
- SECURITY.md (SECURITY.md committed)
- SUPPORT.md (Update SUPPORT.md)

The `README.md` file is expanded, showing the project details:

Project

Welcome to Microsoft Purview Advanced Rich Reports (MPARR) Collector.

Today have the right information in the right moment can be a great business value, we are talking about implement security and compliance, one of the most importance things are understanding that this accomplishment is a business goal, in that order of ideas to have reports business friendly to see how our end users are using and

About

Repository with all the MPARR components solution

- Readme
- MIT license
- Code of conduct
- Security policy

Activity

- 37 stars
- 6 watching
- 6 forks

Report repository

Releases

No releases published

Packages

No packages published

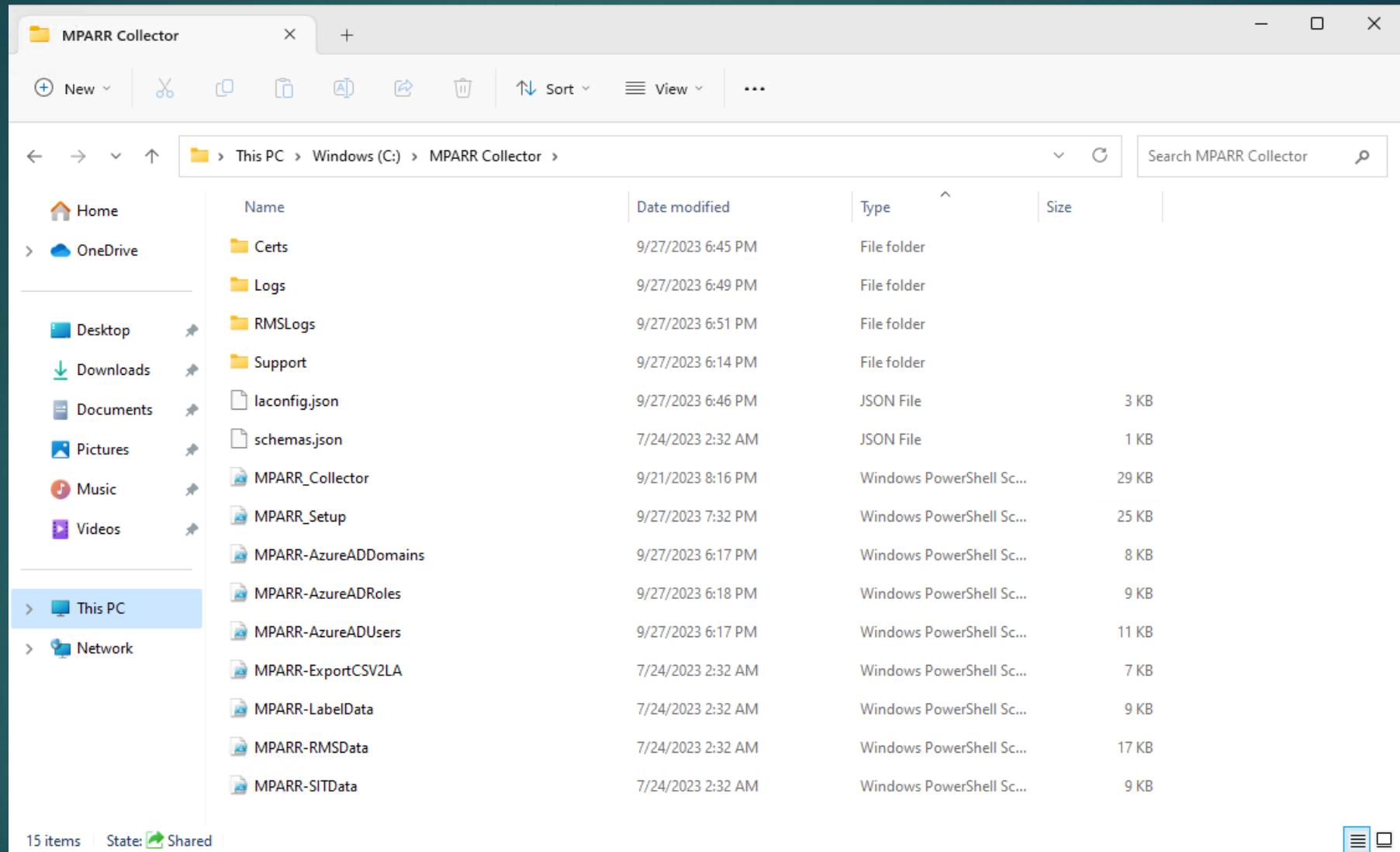
Contributors 4

- ProfKaz Sebastián Zamorano A.
- microsoftopensource Microsoft Open ...
- microsoft-aihub-operations/bot



MPARR Collector

Steps



Run MPARR_Setup.ps1

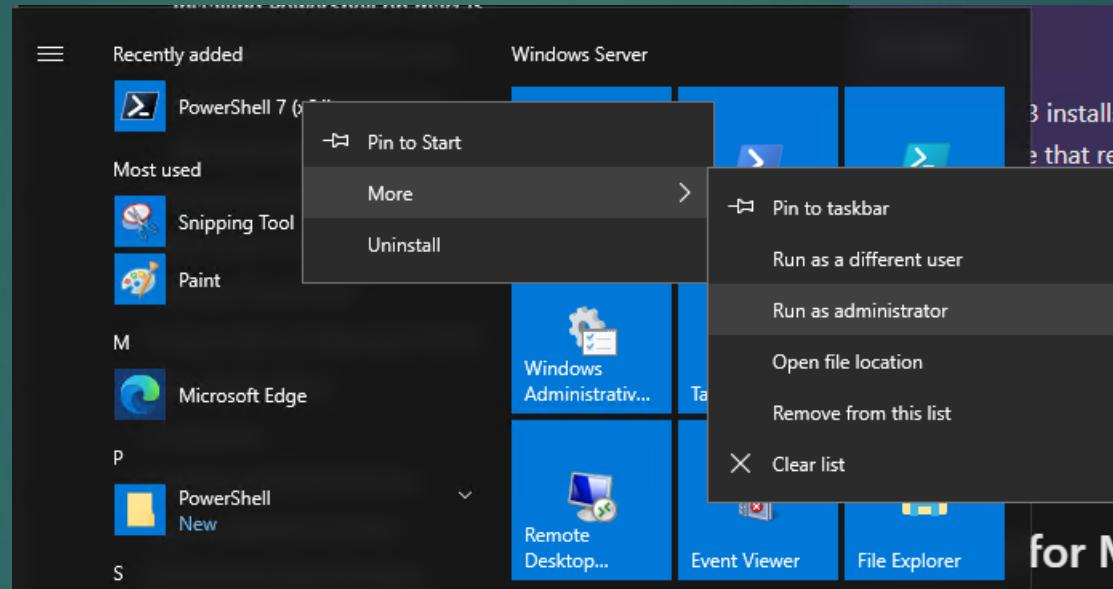
- ▶ Open PowerShell 7 with administrator permissions, if you try with the default PowerShell you will receive a message to use the right one and if you try to execute without administrator rights another message appears about use the right permissions.
- ▶ Move to the folder that contains all the MPARR 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 beginning the script checks 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 automatically exit
- ▶ Execute .\MPARR_Setup.ps1 once again
 - ▶ First the script will validate that all the modules were correctly installed.
 - ▶ Select option 1 to Setup MPARR
 - ▶ You'll be 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 to 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



MPARR Collector

Steps

```
Administrator: PowerShell 7 (x64)
PowerShell 7.3.6
PS C:\Users\Kaz.KAZDEMOS> cd 'C:\MPARR Collector\' 
PS C:\MPARR Collector> .\MPARR_Setup.ps1

Running prerequisites check...

Checking PowerShell version... Passed
    Current version is 7.3.6. Please note that Get-RMSData.ps1 script must be executed under PowerShell 5.1.
Checking PowerShell modules...
    AIPService - Not installed
    Az.Accounts - Not installed
    Az.OperationalInsights - Not installed
    Az.Resources - Not installed
    Microsoft.Graph.Applications - Not installed
    Microsoft.Graph.Users - Not installed
    Microsoft.Graph.Identity.DirectoryManagement - Not installed
    ExchangeOnlineManagement - Not installed
Missing required modules. Proceed with installation?
[Y] Yes [N] No [?] Help (default is "Y"): -
```



Steps

```
Administrator: PowerShell 7 (x64)
Running prerequisites check...

Checking PowerShell version... Passed
    Current version is 7.3.6. Please note that Get-RMSData.ps1 script must be executed under PowerShell 5.1.
Checking PowerShell modules...
    AIPService - Not installed
    Az.Accounts - Not installed
    Az.OperationalInsights - Not installed
    Az.Resources - Not installed
    Microsoft.Graph.Applications - Not installed
    Microsoft.Graph.Users - Not installed
    Microsoft.Graph.Identity.DirectoryManagement - Not installed
    ExchangeOnlineManagement - Not installed
Missing required modules. Proceed with installation?
[Y] Yes [N] No [?] Help (default is "Y"): Y
Installing modules...
    AIPService

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
    Az.Accounts

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
    Az.OperationalInsights

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
    Az.Resources

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
    Az.Resources
Installing package 'Az.Resources' [Copying unzipped package to 'C:\Users\Kaz.KAZDEMONS\AppData\Local\Temp\16287B4519\.']
```

Steps

```
Administrator: Windows PowerShell
Installing module AIPService...
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\Kaz\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): -
```

MPARR Collector

Steps

```
Administrator: C:\Program Files\PowerShell\7\pwsh.exe
PS C:\MPARR Collector> .\MPARR_Setup.ps1

Running prerequisites check...

Checking PowerShell version... Passed
    Current version is 7.3.7. Please note that Get-RMSData.ps1 script must be executed under PowerShell 5.1.
Checking PowerShell modules...
    AIPService - Installed
    Az.Accounts - Installed
    Az.OperationalInsights - Installed
    Az.Resources - Installed
    Microsoft.Graph.Applications - Installed
    Microsoft.Graph.Users - Installed
    Microsoft.Graph.Identity.DirectoryManagement - Installed
    ExchangeOnlineManagement - Installed

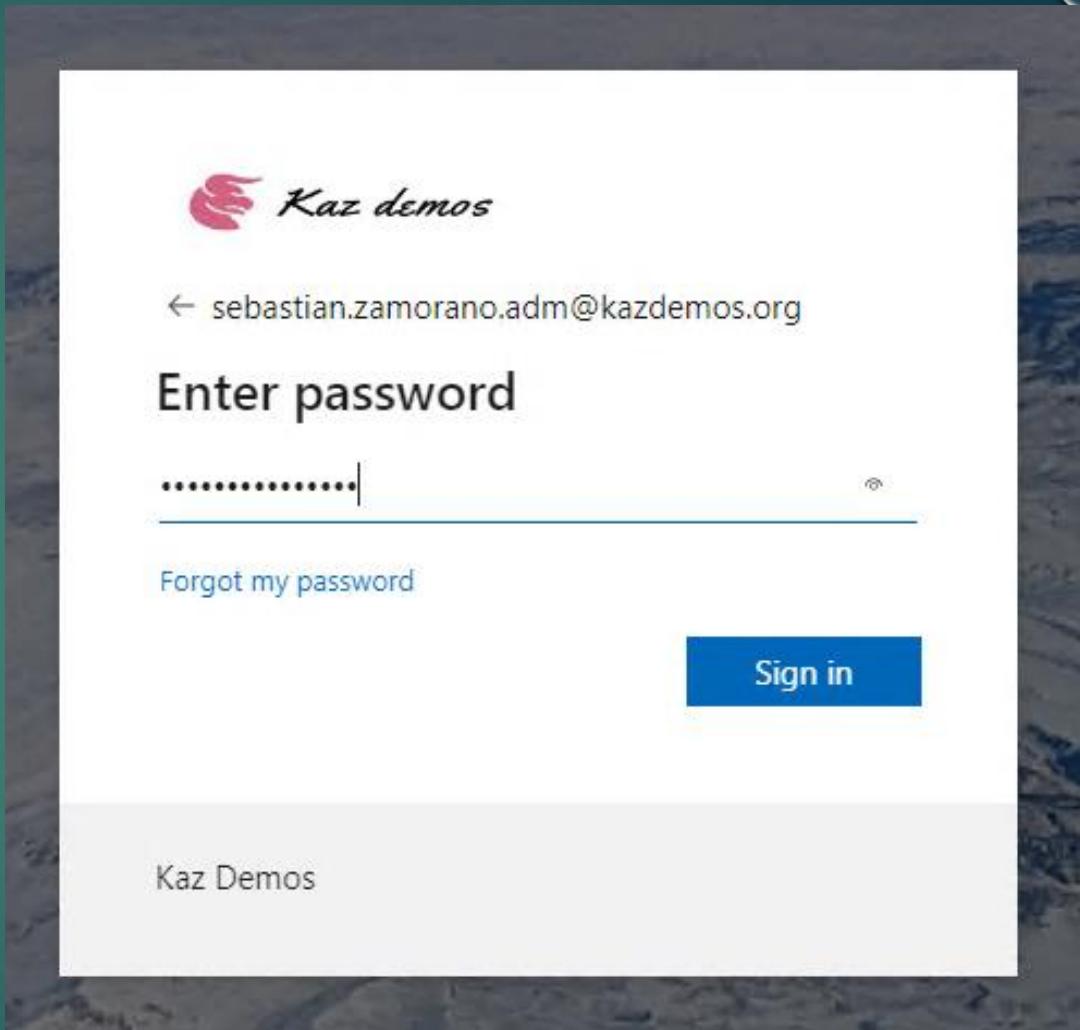
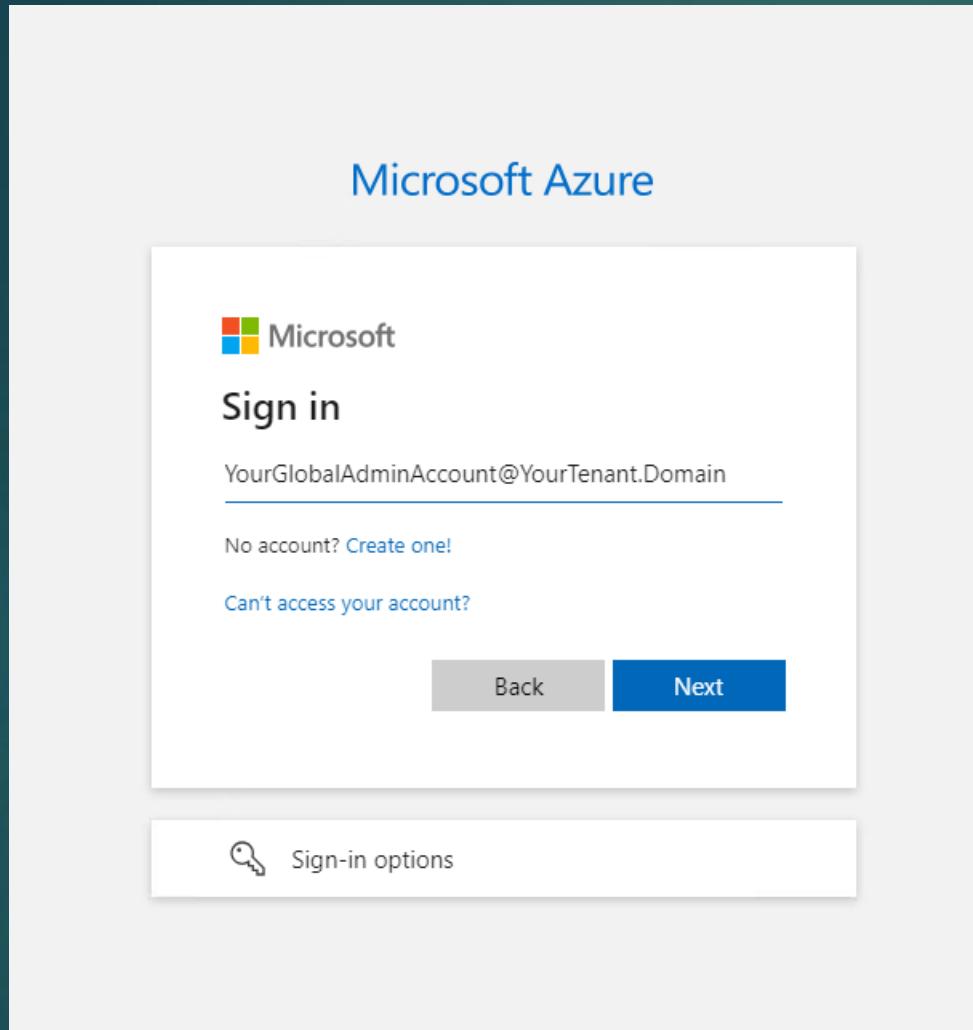
-----
Welcome to the MPARR setup script!
Script allows to automatically execute setup steps.

-----
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:
-
```



Steps



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...

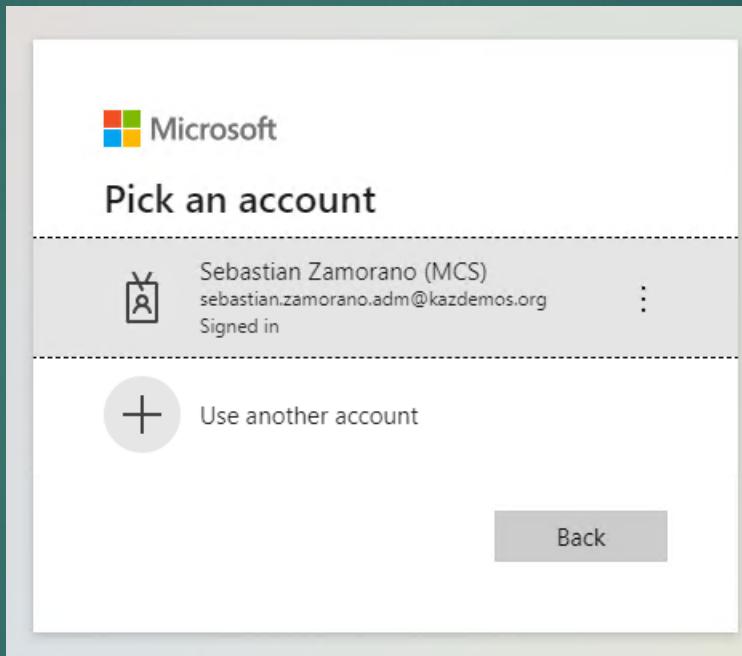
Getting workspaces...
No Name ResourceGroupName Location Sku Tags
----- -----
1 MPARR mparr-demo eastus pergb2018 {}
2 MPARR-Kazdemo mparr-demo eastus pergb2018 {}
3 MPARRData mparr-demo eastus pergb2018 {}

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: -
```



Steps



MPARR Collector

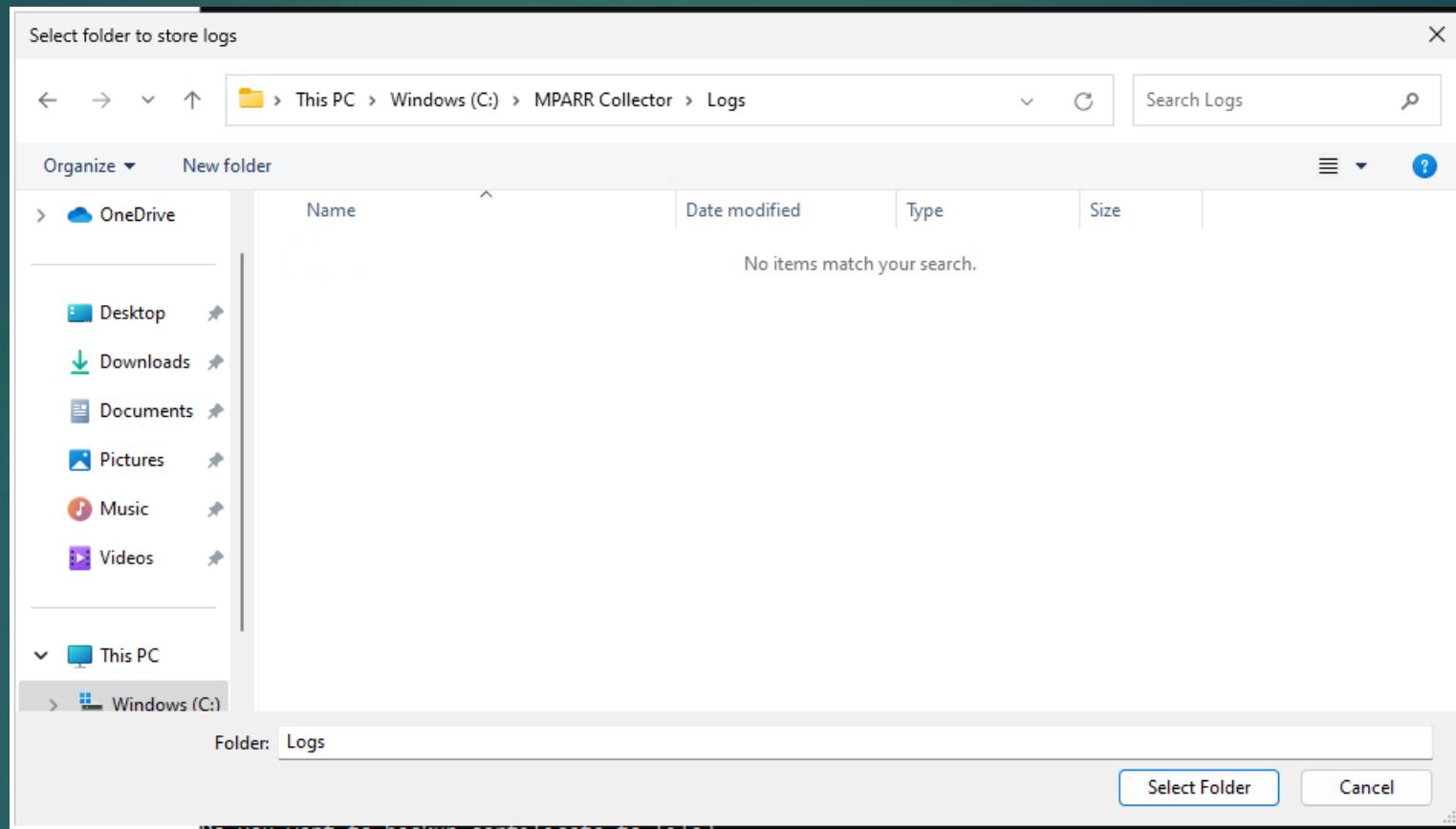
Steps

```
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-b0d8-3fd846b49b8f  
  
Please select cloud version:  
[C] Commercial [G] GCC [H] GCCH [D] DOD [?] Help (default is "C"):
```



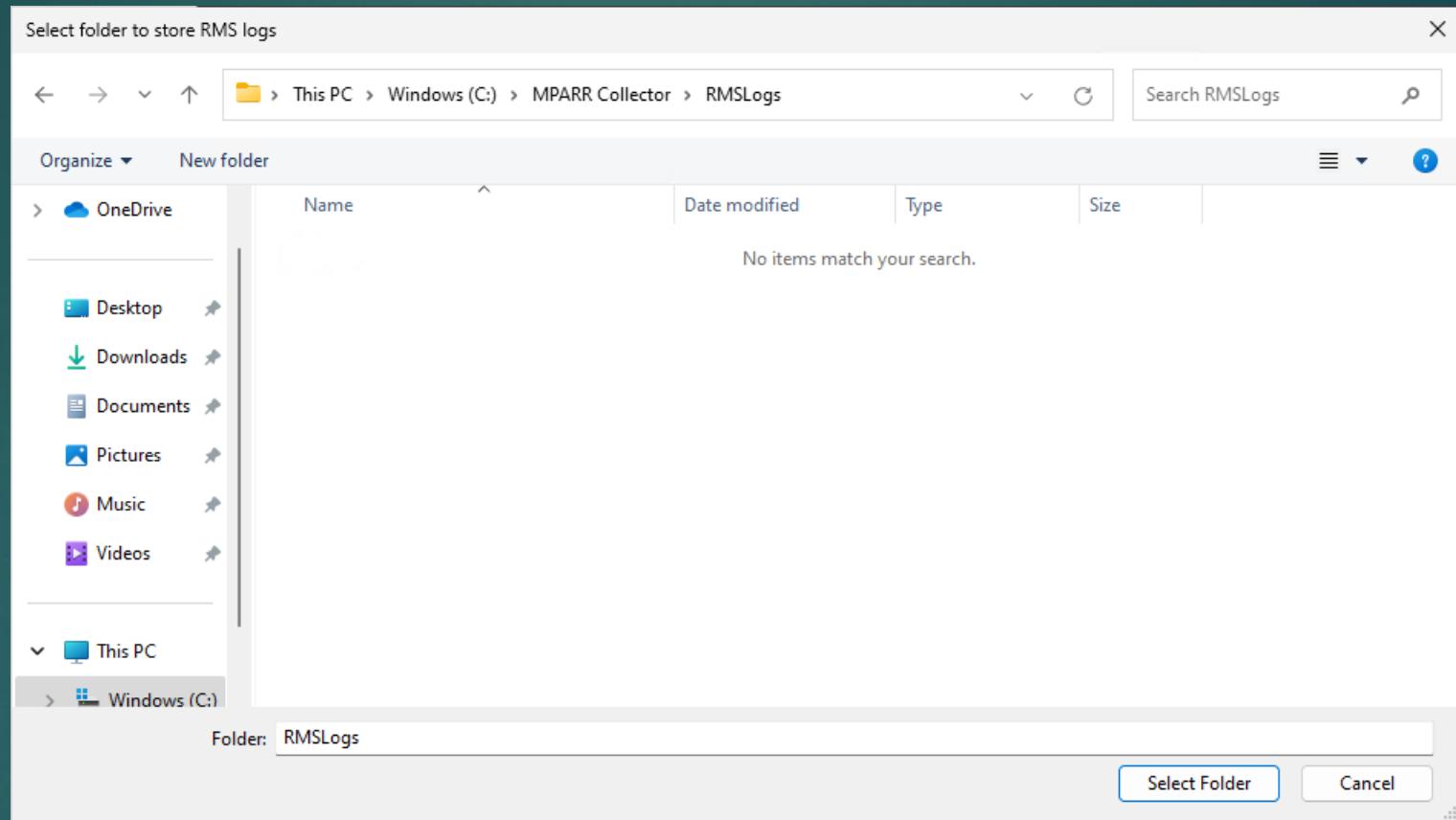
MPARR Collector

Steps



MPARR Collector

Steps



MPARR Collector

Steps

```
Default locations for logs are 'c:\APILogs\RMSLogs\' and 'c:\APILogs\'.
[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.
```



MPARR Collector

Steps

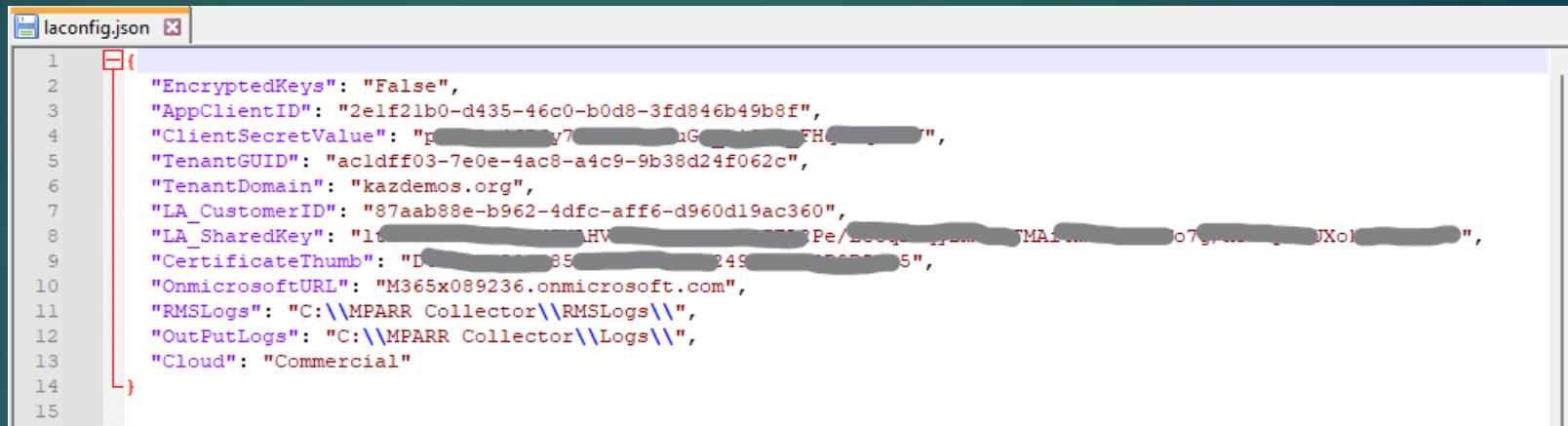
```
What do you want to do?
[1] - Setup MPARR (select LA, register Azure app...)
[2] - Encrypt secrets
[3] - Create scheduled task
[0] - Exit

Please choose option:

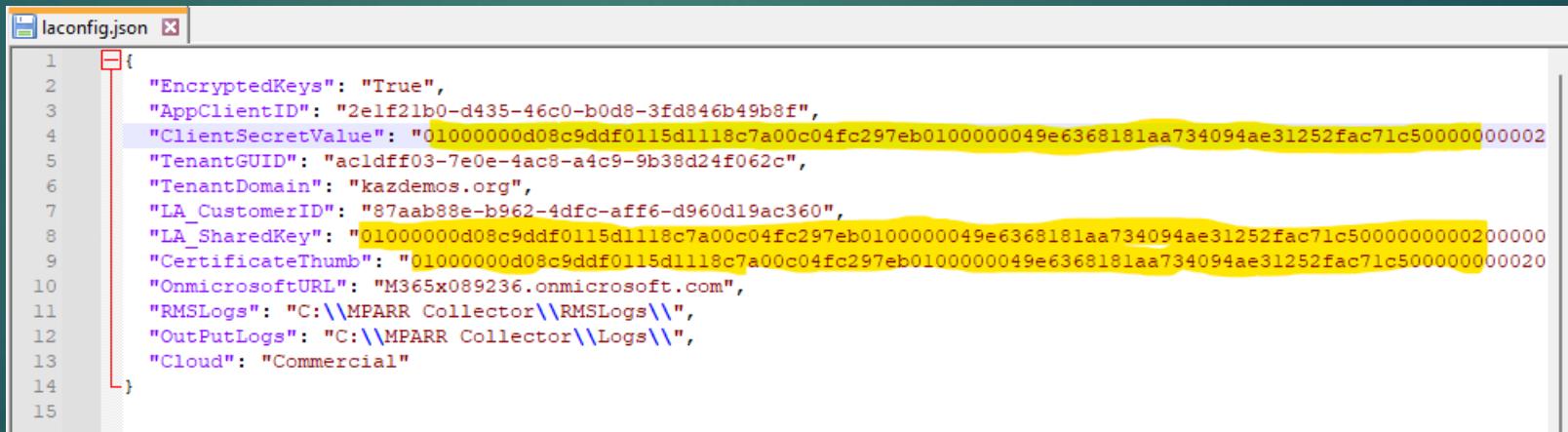
Secrets encrypted.
The old config file moved to 'laconfig_20230928040039.json'
Warning!
Please note that encrypted keys can be decrypted only on this machine, using the same account.
```

MPARR Collector

Steps



```
1 {  
2     "EncryptedKeys": "False",  
3     "AppClientID": "2elf21b0-d435-46c0-b0d8-3fd846b49b8f",  
4     "ClientSecretValue": "p[REDACTED]V7[REDACTED]uG[REDACTED]FH[REDACTED]",  
5     "TenantGUID": "acldff03-7e0e-4ac8-a4c9-9b38d24f062c",  
6     "TenantDomain": "kazdemos.org",  
7     "LA_CustomerID": "87aab88e-b962-4dfc-aff6-d960d19ac360",  
8     "LA_SharedKey": "1t[REDACTED]AHV[REDACTED]Pe/10004-11[REDACTED]TMAi[REDACTED]jo7s[REDACTED]JXo[REDACTED]",  
9     "CertificateThumb": "D:\[REDACTED]85[REDACTED]249[REDACTED]5",  
10    "OnmicrosoftURL": "M365x089236.onmicrosoft.com",  
11    "RMSLogs": "C:\\MPARR Collector\\RMSLogs\\",  
12    "OutPutLogs": "C:\\MPARR Collector\\Logs\\",  
13    "Cloud": "Commercial"  
14 }  
15
```



```
1 {  
2     "EncryptedKeys": "True",  
3     "AppClientID": "2elf21b0-d435-46c0-b0d8-3fd846b49b8f",  
4     "ClientSecretValue": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c50000000002",  
5     "TenantGUID": "acldff03-7e0e-4ac8-a4c9-9b38d24f062c",  
6     "TenantDomain": "kazdemos.org",  
7     "LA_CustomerID": "87aab88e-b962-4dfc-aff6-d960d19ac360",  
8     "LA_SharedKey": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c5000000000200000",  
9     "CertificateThumb": "01000000d08c9ddf0115d1118c7a00c04fc297eb0100000049e6368181aa734094ae31252fac71c500000000020",  
10    "OnmicrosoftURL": "M365x089236.onmicrosoft.com",  
11    "RMSLogs": "C:\\MPARR Collector\\RMSLogs\\",  
12    "OutPutLogs": "C:\\MPARR Collector\\Logs\\",  
13    "Cloud": "Commercial"  
14 }  
15
```



MPARR Collector

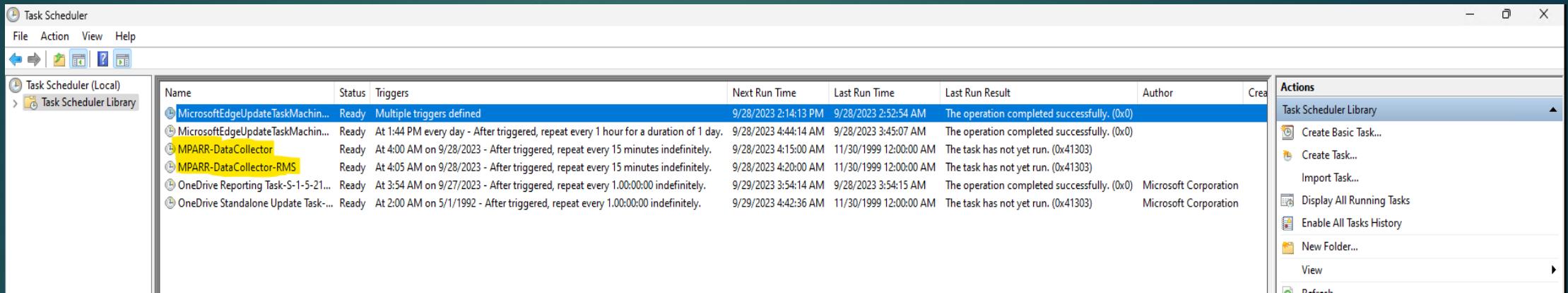
Steps

```
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.
```



MPARR Collector

Steps



The screenshot shows the Windows Task Scheduler window. The left pane displays a tree view with 'Task Scheduler (Local)' selected at the top level, and 'Task Scheduler Library' expanded. The right pane is a grid view of tasks, with the first task, 'MicrosoftEdgeUpdateTaskMachine...', highlighted by a yellow selection bar. The columns in the grid are: Name, Status, Triggers, Next Run Time, Last Run Time, Last Run Result, Author, and Create. The 'Actions' pane on the right lists various options: Task Scheduler Library, Create Basic Task..., Create Task..., Import Task..., Display All Running Tasks, Enable All Tasks History, New Folder..., View, and Refresh.

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Create
MicrosoftEdgeUpdateTaskMachine...	Ready	Multiple triggers defined	9/28/2023 2:14:13 PM	9/28/2023 2:52:54 AM	The operation completed successfully. (0x0)		
MicrosoftEdgeUpdateTaskMachine...	Ready	At 1:44 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	9/28/2023 4:44:14 AM	9/28/2023 3:45:07 AM	The operation completed successfully. (0x0)		
MPARR-DataCollector	Ready	At 4:00 AM on 9/28/2023 - After triggered, repeat every 15 minutes indefinitely.	9/28/2023 4:15:00 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)		
MPARR-DataCollector-RMS	Ready	At 4:05 AM on 9/28/2023 - After triggered, repeat every 15 minutes indefinitely.	9/28/2023 4:20:00 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)		
OneDrive Reporting Task-S-1-5-21...	Ready	At 3:54 AM on 9/27/2023 - After triggered, repeat every 1:00:00 indefinitely.	9/29/2023 3:54:14 AM	9/28/2023 3:54:15 AM	The operation completed successfully. (0x0)	Microsoft Corporation	
OneDrive Standalone Update Task-...	Ready	At 2:00 AM on 5/1/1992 - After triggered, repeat every 1:00:00 indefinitely.	9/29/2023 4:42:36 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	



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**

MPARR Setup final steps

Steps

Microsoft Azure Search resources, services, and docs (G+/-) Home > Kaz Demos | Overview sebastian.zamorano.ad... KAZ DEMOS (KAZDEMONS.ORG)

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

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	Kaz Demos	Users	50,065
Tenant ID	ac1dff03-7e0e-4ac8-a4c9-9b38d24f062c	Groups	80
Primary domain	kazdemos.org	Applications	10
License	Microsoft Entra ID P2	Devices	23

Alerts

Microsoft Entra Connect v1 Retirement
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

[Learn more](#)

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

[Learn more](#)

Upcoming MFA Server deprecation
Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.

[Learn more](#)

Migrate to the converged Authentication methods policy
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2024 to avoid any service impact.

[Learn more](#)

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectory...

MPARR Setup final steps

Steps

Screenshot of the Microsoft Azure portal showing the App registrations page for the "Kaz Demos" tenant.

The page title is "Kaz Demos | App registrations". The left sidebar shows the following navigation:

- Overview
- Preview features
- Diagnose and solve problems
- Manage
 - Users
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Delegated admin partners
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance
 - Application proxy
 - Custom security attributes

The "App registrations" link is highlighted in the sidebar.

The main content area shows a message: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph." A "Learn more" link is provided.

The "Owned applications" tab is selected. The table lists the following application details:

Display name	Application (client) ID	Created on	Certificates & secrets
MIP-Scanner	cab9530a-5b06-4c61-b09b-590fd6a40f8	11/15/2022	Current
MPARR-Data	2e1f21b0-d435-46c0-b0d8-3fd846b49b8f	9/28/2023	Current
MPARR-DataCollector-6c3a4b07	aef5a2f3-4ee5-4719-a5cd-e93785b0088d	9/25/2023	Current
MPARR-DataCollector-807c7965	f9423a4d-d05d-41a6-a5f8-805b54fa134d	9/28/2023	Current
MPARR - Collector for Sentinel	096e413e-71b4-4092-a0c0-d97314790ef9	12/12/2022	Current

MPARR Setup final steps

Steps

Microsoft Azure Search resources, services, and docs (G+) sebastian.zamorano.ad... KAZ DEMOS (KAZDEMONS.ORG)

Home > Kaz Demos | App registrations > MPARR-Data

MPARR-Data | API permissions

Search Refresh Got feedback?

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

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

Add a permission Grant admin consent for Kaz Demos

API / Permissions name	Type	Description	Admin consent requ...	Status
Application.Read.All	Application	Read all service configuration and log data for the Azure I...	Yes	⚠️ Not granted for Kaz De...
AuditLog.Read.All	Application	Read all audit log data	Yes	⚠️ Not granted for Kaz De...
Directory.Read.All	Application	Read directory data	Yes	⚠️ Not granted for Kaz De...
Group.Read.All	Application	Read all groups	Yes	⚠️ Not granted for Kaz De...
Organization.Read.All	Application	Read organization information	Yes	⚠️ Not granted for Kaz De...
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠️ Not granted for Kaz De...
Exchange.ManageAsApp	Application	Manage Exchange As Application	Yes	⚠️ Not granted for Kaz De...
ActivityFeed.Read	Application	Read activity data for your organization	Yes	⚠️ Not granted for Kaz De...
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	⚠️ Not granted for Kaz De...
ServiceHealth.Read	Application	Read service health information for your organization	Yes	⚠️ Not granted for Kaz De...

MPARR Setup final steps

Steps

Microsoft Azure Search resources, services, and docs (G+)

Home > Kaz Demos | App registrations > MPARR-Data

MPARR-Data | API permissions

Search Refresh Got feedback? sebastian.zamorano.ad... KAZ DEMOS (KAZDEMOS.ORG)

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

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

Add a permission Grant admin consent for Kaz Demos

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

MPARR Setup final steps

Steps

Screenshot of the Windows Task Scheduler application showing scheduled tasks.

The Task Scheduler window displays the following tasks:

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
MicrosoftEdgeUpdateTaskMachineCore(C322229E-0...	Ready	Multiple triggers defined	9/28/2023 2:14:13 PM	9/28/2023 7:25:28 AM	The operation completed successfully. (0)
MicrosoftEdgeUpdateTaskMachineUA(558AD065-42...	Ready	At 1:44 PM every day - After trigger...	9/28/2023 9:44:14 AM	9/28/2023 8:44:15 AM	The operation completed successfully. (0)
MPARR-DataCollector	Ready	At 9:00 AM on 9/28/2023 - After tri...	9/28/2023 9:15:00 AM	9/28/2023 9:10:18 AM	The operation completed successfully. (0)
MPARR-DataCollector-RMS	Ready	At 9:05 AM on 9/28/2023 - After tri...	9/28/2023 9:20:00 AM	9/28/2023 9:11:05 AM	The operation completed successfully. (0)
OneDrive Reporting Task-S-1-5-21-2189507727-1341...	Ready	At 12:40 PM on 9/22/2023 - After tri...	9/28/2023 12:40:02 PM	9/25/2023 12:40:03 PM	The operation completed successfully. (0)
OneDrive Standalone Update Task-S-1-5-21-2189507...	Ready	At 11:00 AM on 5/1/1992 - After tri...	9/28/2023 1:53:14 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)

The Actions pane on the right shows the following options:

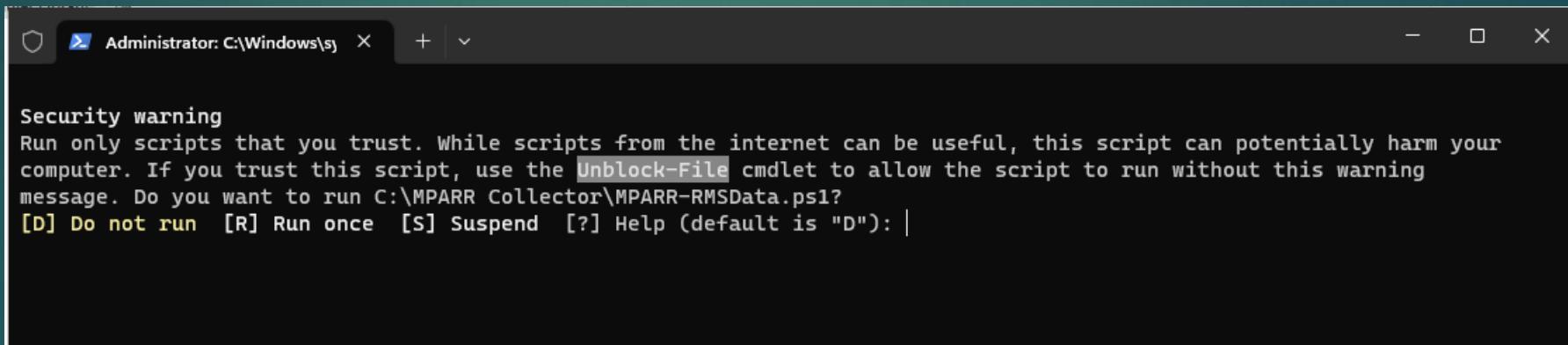
- Task Scheduler Library
- Create Basic Task...
- Create Task...
- Import Task...
- Display All Running Tasks
- Disable All Tasks History
- New Folder...
- View
- Refresh
- Help

Selected Items: MPARR-DataCollector

- Run
- End
- Disable
- Delete
- Help

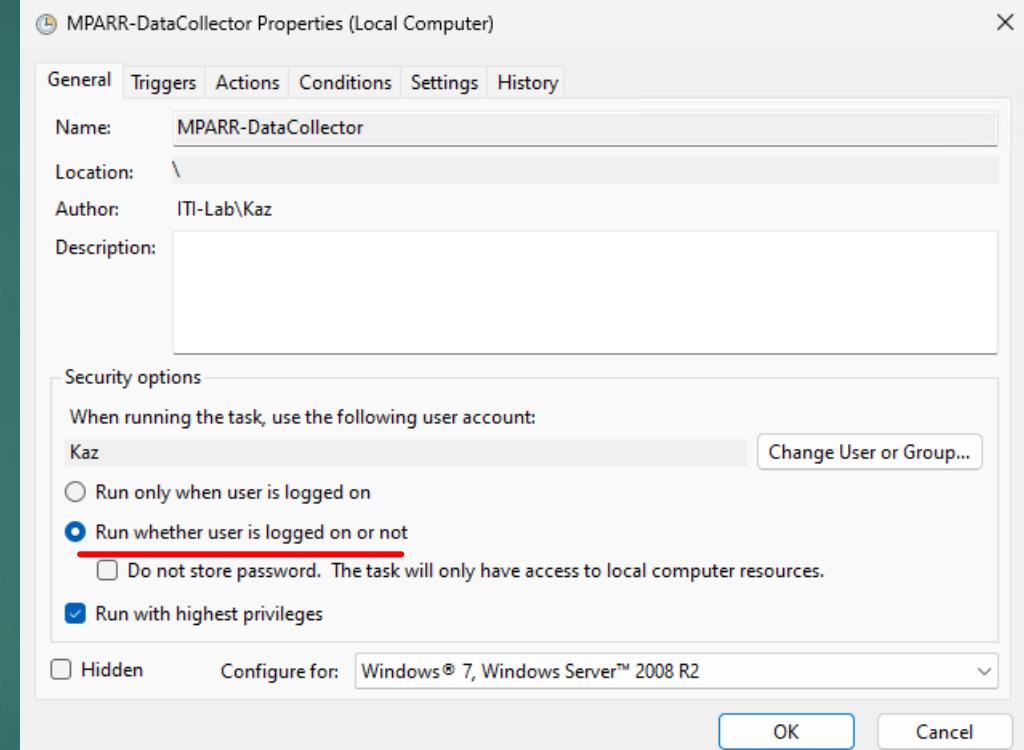
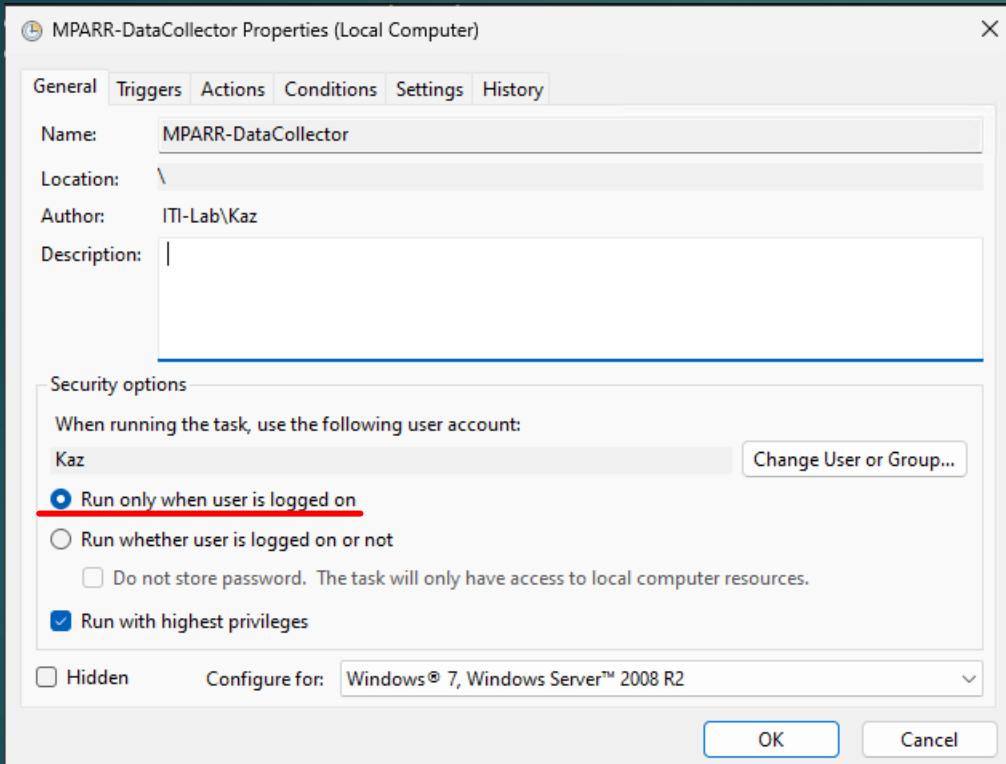
MPARR Setup final steps

Steps



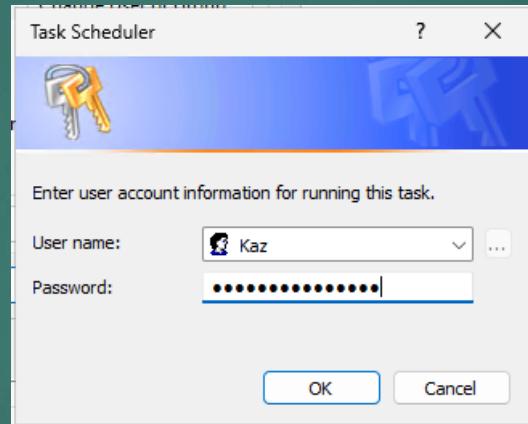
MPARR Setup final steps

Steps



MPARR Setup final steps

Steps



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.

Compliance Admin Role for Script

Steps

The screenshot shows the Microsoft Azure portal interface with a search bar at the top containing "Microsoft Entra". Below the search bar, there are several navigation tabs: All, Services (32), Marketplace (3), Documentation (99+), Resources (0), and Resource Groups (0). The "All" tab is selected. Under the "Services" section, "Microsoft Entra ID" is highlighted. Other services listed include Microsoft Entra Connect, Microsoft Entra ID Protection, Microsoft Entra ID risk detections, and Microsoft Entra ID risky sign-ins. In the "Marketplace" section, there are links to Microsoft Entra Digital IAM Managed Service and Omada Identity Cloud. The "Documentation" section contains links to Microsoft Entra Permissions Management Quickstart Guide, Authorize access with Microsoft Entra ID for Azure SignalR Service, How to apply Conditional Access policies to Microsoft Entra Privat..., Workload identities - Microsoft Entra, Quickstart - Set up a tenant - Microsoft Entra, Download a list of users in the Azure portal - Microsoft Entra, Authorize request to Web PubSub resources with Microsoft Entra ..., and Authorize requests to SignalR resources with Microsoft Entra appl.... At the bottom of the page, there are sections for "See all" and "Navigate". On the right side, there is a sidebar with a profile picture for "sebastian.zamorano.ad..." and "KAZ DEMOS (KAZDEMONS.ORG)". The sidebar also includes a "More services" link and a "Viewed" section with a list of items viewed recently, such as "minutes ago", "ours ago", "hours ago", "days ago", "ays ago", "ays ago", "week ago", and "2 weeks ago".

Compliance Admin Role for Script

Steps

Microsoft Azure Search resources, services, and docs (G+/-) Add Manage tenants What's new Preview features Got feedback? sebastian.zamorano.ad... KAZ DEMOS (KAZDEMONS.ORG)

Home > Kaz Demos | Overview Microsoft Entra ID

Overview Preview features Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators**
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes
- Licenses
- Cross-tenant synchronization
- Microsoft Entra Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	Kaz Demos	Users	50,065
Tenant ID	ac1dff03-7e0e-4ac8-a4c9-9b38d24f062c	Groups	80
Primary domain	kazdemos.org	Applications	10
License	Microsoft Entra ID P2	Devices	23

Alerts

Microsoft Entra Connect v1 Retirement
All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

[Learn more](#)

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

[Learn more](#)

Upcoming MFA Server deprecation
Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.

[Learn more](#)

Migrate to the converged Authentication methods policy
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2024 to avoid any service impact.

[Learn more](#)

[https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/...](https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/)

Compliance Admin Role for Script

Steps

Screenshot of the Microsoft Azure Roles and administrators page showing the list of built-in roles.

The Compliance Administrator role is selected.

Role	Description	Assignments	Type
B2C IEF Keyset Administrator	Framework (IEF).	0	Built-in
B2C IEF Policy Administrator	Can create and manage trust framework policies in the Identity Experience Framework (IEF).	0	Built-in
Billing Administrator	Can perform common billing related tasks like updating payment information.	0	Built-in
Cloud App Security Administrator	Can manage all aspects of the Cloud App Security product.	0	Built-in
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	0	PRIVILEGED
Cloud Device Administrator	Limited access to manage devices in Azure AD.	0	PRIVILEGED
Compliance Administrator	Can read and manage compliance configuration and reports in Azure AD and Microsoft 365.	17	Built-in
Compliance Data Administrator	Creates and manages compliance content.	0	Built-in
Conditional Access Administrator	Can manage Conditional Access capabilities.	0	PRIVILEGED
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	0	Built-in
Desktop Analytics Administrator	Can access and manage Desktop management tools and services.	0	Built-in
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	2	Built-in
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	0	PRIVILEGED
Domain Name Administrator	Can manage domain names in cloud and on-premises.	0	Built-in
Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.	0	Built-in
Edge Administrator	Manage all aspects of Microsoft Edge.	0	Built-in
Exchange Administrator	Can manage all aspects of the Exchange product.	0	Built-in
Exchange Recipient Administrator	Can create or update Exchange Online recipients within the Exchange Online organization.	0	Built-in
Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.	0	Built-in
External ID User Flow Administrator	Can create and manage all aspects of user flows.	0	Built-in
File + HD User Flow Administrator	Can create and manage all aspects of user flows.	0	Built-in

Compliance Admin Role for Script

Steps

Home >

Compliance Administrator | Assignments

Privileged Identity Management | Azure AD roles

Add assignments Settings Refresh Export Got feedback?

Manage

Assignments Description Role settings

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

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



Compliance Admin Role for Script

Steps

Microsoft Azure Search resources, services, and docs (G+) sebastian.zamorano.ad... KAZ DEMOS (KAZDEMONS.ORG)

Home > Kaz Demos | Roles and administrators > Role

Add assignments ...

Privileged Identity Management | Azure AD roles

Membership Setting

You can also assign roles to groups now. [Learn more](#)

Resource Kaz Demos

Resource type Directory

Select role ⓘ [Compliance Administrator](#)

Scope type ⓘ [Directory](#)

Select member(s) * ⓘ No member selected

Select a member

Privileged Identity Management | Azure AD roles

Try changing or adding filters if you don't see what you're looking for.

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

Search

All Users Groups Enterprise applications

	Name	Type	Details
<input type="checkbox"/>	MPARR - Collector for Sentinel	Enterprise ap...	[REDACTED]
<input type="checkbox"/>	MPARR-DataCollector-6c3a4b07	Enterprise ap...	[REDACTED]
<input checked="" type="checkbox"/>	MPARR-DataCollector-807c7965	Enterprise ap...	[REDACTED]
<input type="checkbox"/>	MPARR-PurviewDataMap	Enterprise ap...	[REDACTED]
<input type="checkbox"/>	MPARRCollector	Enterprise ap...	[REDACTED]

Selected (1)

Reset

MPARR-DataCollector-807c7965 [REDACTED] 4d Remove

Next > Cancel Select

The screenshot shows the Microsoft Azure Privileged Identity Management interface. A modal window titled 'Select a member' is open, showing a list of Azure AD roles. The user has selected the 'Compliance Administrator' role for the 'MPARR-DataCollector-807c7965' enterprise application. The 'Selected (1)' section shows the chosen item. The background shows the 'Add assignments' page with the 'Membership' tab selected, and the 'Resource' dropdown set to 'Kaz Demos'.



Compliance Admin Role for Script

Steps

Home > Compliance Administrator | Assignments >

Add assignments ...

Privileged Identity Management | Azure AD roles

Membership Setting

Assignment type ⓘ
 Eligible
 Active

Maximum allowed assignment duration is permanent.

Permanently assigned

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

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

Enter justification *

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



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-IPPSession
167     Connect-IPPSession -CertificateThumbPrint $CertificateThumb -AppID $AppClientID -Organization $OnmicrosoftTenant
```



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*



Workstation - PowerShell

STEPS

```
Administrator: PowerShell X + | - □ ×
PS C:\MPARR Collector> .\MPARR-LabelData.ps1

-----
We have made updates to move the SCC admin experience to REST-based APIs. In doing so, we will be deprecating the legacy
Remote PowerShell (RPS) protocol starting July 15, 2023.

Benefits of REST-based cmdlets: improved security, WinRM no longer required for client-server communication, improved er
ror handling.

The REST API has the same cmdlets available and feature parity with RPS(V1) cmdlets, so existing scripts and processes d
on't need to be updated. Simply using the new module will ensure REST is used rather than RPS.

For more information, go to https://aka.ms/exov3-module
-----
54 rows returned by Get-Label
54 rows written to Log Analytics workspace https://7543218a-8c3e-457d-870a-683171ad44d4.ods.opinsights.azure.com/api/
logs?api-version=2016-04-01
PS C:\MPARR Collector>
```



Workstation - PowerShell

STEPS

```
Administrator: PowerShell X + - □ ×
PS C:\MPARR Collector> .\MPARR-SITData.ps1
-----
We have made updates to move the SCC admin experience to REST-based APIs. In doing so, we will be deprecating the legacy
Remote PowerShell (RPS) protocol starting July 15, 2023.

Benefits of REST-based cmdlets: improved security, WinRM no longer required for client-server communication, improved er
ror handling.

The REST API has the same cmdlets available and feature parity with RPS(V1) cmdlets, so existing scripts and processes d
on't need to be updated. Simply using the new module will ensure REST is used rather than RPS.

For more information, go to https://aka.ms/exov3-module
-----
402 rows returned by Get-DlpSensitiveInformationType
402 rows written to Log Analytics workspace https://7543218a-8c3e-457d-870a-683171ad44d4.ods.opinsights.azure.com/api
/logs?api-version=2016-04-01
PS C:\MPARR Collector> |
```



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-IPPSession
167     Connect-IPPSession -CertificateThumbPrint $CertificateThumb -AppID $AppClientID -Organization $onmicrosoftTenant
```



Create a Table in Logs Analytics with Product names and service plan identifiers for licensing

- ▶ When user licensing data is exported, a special names are used and doesn't match with Known products, these steps helps to create a Matrix for that purpose.
- ▶ Download the latest updated product list from [here](#) and save the file in a known folder.
- ▶ Using the script ExportCSV2LA.ps1 you can import the data to Logs Analytics, to do that, execute the script in this way:

```
PS C:\Collector> .\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>

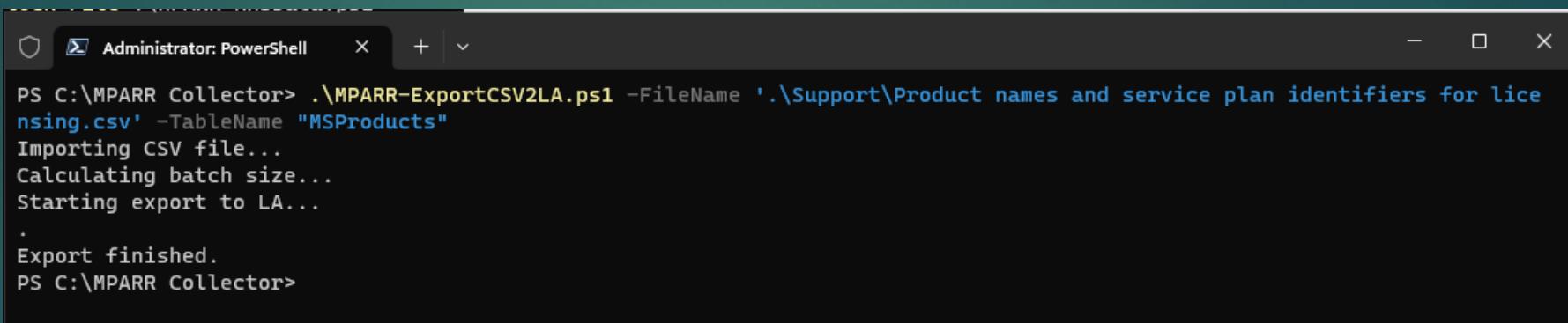
**Depending on the Logs Analytics workspace retention this script will be required to execute continuously(monthly for a 30 days retention period) to don't lose that information

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



Import Data to Logs Analytics

STEPS



```
PS C:\MPARR Collector> .\MPARR-ExportCSV2LA.ps1 -FileName '.\Support\Product names and service plan identifiers for licensing.csv' -TableName "MSProducts"
Importing CSV file...
Calculating batch size...
Starting export to LA...
.
Export finished.
PS C:\MPARR Collector>
```



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
```

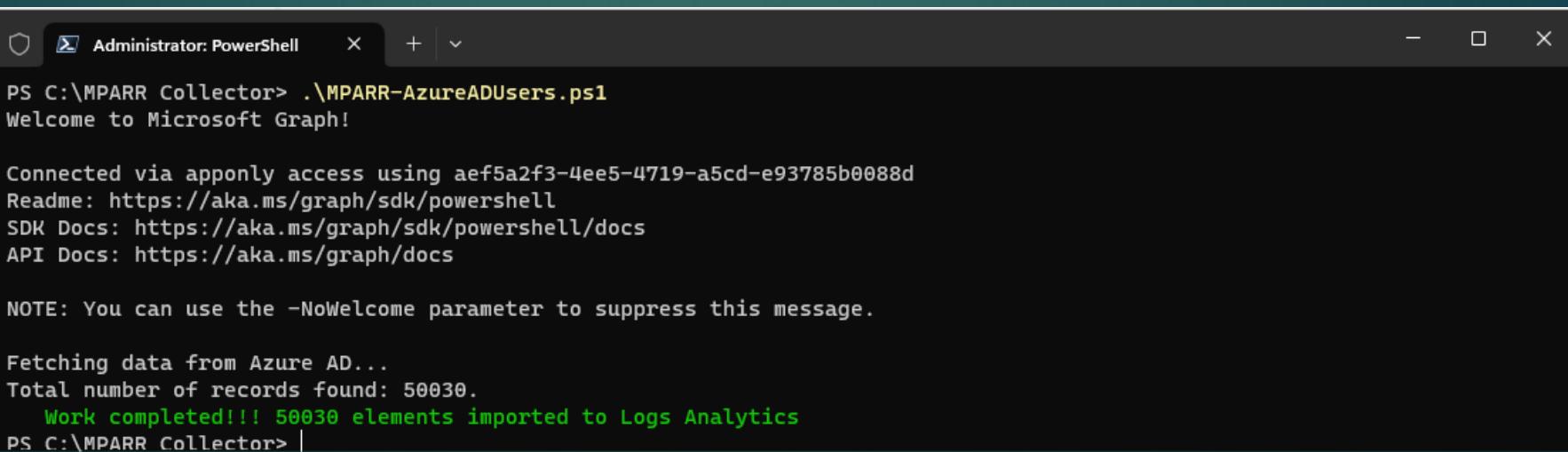
- How to validate the data in Logs Analytics, [click here](#).

*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



Powershell – Microsoft Users

STEPS



```
Administrator: PowerShell
PS C:\MPARR Collector> .\MPARR-AzureADUsers.ps1
Welcome to Microsoft Graph!

Connected via apponly access using aef5a2f3-4ee5-4719-a5cd-e93785b0088d
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.

Fetching data from Azure AD...
Total number of records found: 50030.
Work completed!!! 50030 elements imported to Logs Analytics
PS C:\MPARR Collector>
```



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

```
Administrator: PowerShell
PS C:\MPARR Collector> .\MPARR-AzureADDomains.ps1
Welcome to Microsoft Graph!

Connected via apponly access using aef5a2f3-4ee5-4719-a5cd-e93785b0088d
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.

    3 rows returned by Get-MgDomains
Processing account M365x089236.onmicrosoft.com 1/3
Processing account kazdemos.org 2/3
Processing account ms-mparr.com 3/3
    3 rows written to Log Analytics workspace https://7543218a-8c3e-457d-870a-683171ad44d4.ods.opinsights.azure.com/api/logs?api-version=2016-04-01
PS C:\MPARR Collector> |
```



Powershell – Microsoft Entra ID

STEPS

```
Administrator: PowerShell PS C:\MPARR Collector> .\MPARR-AzureADRoles.ps1
Welcome to Microsoft Graph!

Connected via apponly access using aef5a2f3-4ee5-4719-a5cd-e93785b0088d
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.

    18 rows returned by Get-MgDirectoryRole
Processing account Conditional Access Administrator 1/18
Processing account Privileged Role Administrator 2/18
Processing account Exchange Administrator 3/18
Processing account Teams Administrator 4/18
Processing account Cloud Device Administrator 5/18
Processing account Security Administrator 6/18
Processing account Global Reader 7/18
Processing account Intune Administrator 8/18
Processing account Security Reader 9/18
Processing account User Administrator 10/18
Processing account Reports Reader 11/18
Processing account Compliance Administrator 12/18
Processing account Azure Information Protection Administrator 13/18
Processing account Directory Readers 14/18
Processing account Global Administrator 15/18
Processing account Application Administrator 16/18
Processing account Azure AD Joined Device Local Administrator 17/18
Processing account Cloud App Security Administrator 18/18
    18 rows written to Log Analytics workspace https://7543218a-8c3e-457d-870a-683171ad44d4.ods.opinsights.azure.com/api/logs?api-version=2016-04-01
PS C:\MPARR Collector>
```



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**
 - ▶ **MSPProducts_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.*



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
```

Logs Analytics workspace

Steps

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

Services

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

Marketplace

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

Documentation

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



Logs Analytics workspace

Steps

The screenshot shows the 'Log Analytics workspaces' page in the Azure portal. The top navigation bar includes 'Home >', the workspace name 'Log Analytics workspaces', and a user icon 'mscompliance'. Below the navigation are standard toolbar buttons: '+ Create', 'Open recycle bin', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A search bar contains the text 'Sentinel'. Filter options include 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. On the right, grouping and view settings are shown: 'No grouping' and 'List view'. The main table displays one workspace entry:

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



Logs Analytics workspace

Steps

Home > Log Analytics workspaces >

Log Analytics workspace

mscompliance

+ Create Open recycle bin ...

Sentinel

Name ↑↓

Sentinel

...

Search

SENTINEL Log Analytics workspace

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Agents management

Legacy agents management

Custom logs

Computer Groups

Data export

Linked storage accounts

Network isolation

Tables

General

Workspace summary

Workbooks

Logs

Solutions

Delete

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

Resource group (move) : lab

Status : Active

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : 1c2f1111-1111-1111-1111-111111111111

Tags (edit) : Click here to add tags

Get started with Log Analytics

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

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)
Windows and Linux Agents management
Storage account log
System Center Operations Manager

2 Configure monitoring solutions

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

View solutions

Maximize your Log Analytics experience



Logs Analytics workspace

Steps

The screenshot shows the Microsoft Sentinel Log Analytics workspace interface. On the left, a sidebar menu is open under the 'Logs' section, which is highlighted with a yellow background. Other sections like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems' are also listed. The main area displays a 'New Query 1' window with a search bar, a 'Tables' tab selected, and a list of favorite logs including 'LogManagement', 'Microsoft Sentinel', and 'Custom Logs'. Below this is a 'Queries History' section listing several log queries with their execution details and a 'Run' button.

Sentinel | Logs
Log Analytics workspace

New Query 1

Tables Queries Functions ...

Time range : Last 24 hours

Feedback Queries Format query

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

Settings

- Locks
- Agents management
- Legacy agents management
- Custom logs
- Computer Groups
- Data export
- Linked storage accounts
- Network isolation
- Tables
- General
- Workspace summary
- Workbooks
- Logs
- Solutions
- Usage and estimated costs
- Properties
- Service Map

Favorites

You can add favorites by clicking on the star icon

LogManagement

Microsoft Sentinel

Custom Logs

- AuditAzureActiveDirectory_CL
- AuditExchange_CL
- AuditGeneral_CL
- AuditSharePoint_CL
- AzureADDomains_CL
- AzureADRoles_CL
- AzureADUsers_CL
- DLPAll_CL
- Labels_CL
- MSProducts_CL
- RMSData_CL
- RMSDataDetails_CL

Queries History

- DLPAII_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation_s) by Operation_s
1/30/2023, 1:23 PM | 4 results Run
- AuditSharePoint_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation_s) by Operation_s
1/30/2023, 1:22 PM | 47 results Run
- AuditGeneral_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation_s) by Operation_s
1/30/2023, 1:21 PM | 95 results Run
- AuditExchange_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation_s) by Operation_s
1/30/2023, 1:20 PM | 33 results Run
- AuditAzureActiveDirectory_CL | where TimeGenerated > now(-730d) | summarize dcount(Operation_s) by Operation_s
1/30/2023, 1:14 PM | 38 results Run
- Labels_CL
1/27/2023, 3:38 PM | 422 results Run

Logs Analytics workspace

Latest time where activities are log

Microsoft Azure Search resources, services, and docs (G+) Home > MPARR sebastian.zamorano@iti... ITI (ITIMWLABA.CLICK)

MPARR | Logs

Log Analytics workspace

New Query 1* New Query 2* +

MPARR Select scope Run Time range : Set in query Save Share New alert rule Export Pin to Format query ...

Tables Queries Functions ...

Search Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the star icon

- LogManagement
- Custom Logs
 - AuditAzureActiveDirectory_CL
 - AuditExchange_CL
 - AuditGeneral_CL
 - AuditSharePoint_CL
 - AzureADDomains_CL
 - AzureADRoles_CL
 - AzureADUsers_CL
 - Labels_CL
 - RMSData_CL
 - RMSDataDetails_CL

1 AuditGeneral_CL
2 | where TimeGenerated > now(-1d)
3 | summarize by
4 Year = datetime_part('Year',TimeGenerated),
5 Month = datetime_part('Month',TimeGenerated),
6 Day = datetime_part('Day',TimeGenerated),
7 Hour = datetime_part('Hour',TimeGenerated)

Results Chart

Year	Month	Day	Hour ↑↓
> 2023	9	28	0
> 2023	9	28	1
> 2023	9	28	2
> 2023	9	28	3
> 2023	9	28	4
> 2023	9	28	5
> 2023	9	28	6
> 2023	9	28	7
> 2023	9	28	8
> 2023	9	28	9
> 2023	9	28	10

Columns

Logs Analytics workspace

Activities collect in AuditGeneral_CL in the last day

Microsoft Azure Search resources, services, and docs (G+) sebastian.zamorano@iti...
ITI (ITIMWLABA.CLICK)

Home > MPARR

MPARR | Logs Log Analytics workspace

New Query 1* New Query 2* + Feedback Queries ...

MPARR Select scope Run Time range: Set in query Save Share New alert rule Export Pin to Format query ...

Tables Queries Functions ... <

Search Filter Group by: Solution

Collapse all

Favorites You can add favorites by clicking on the star icon

LogManagement

Custom Logs

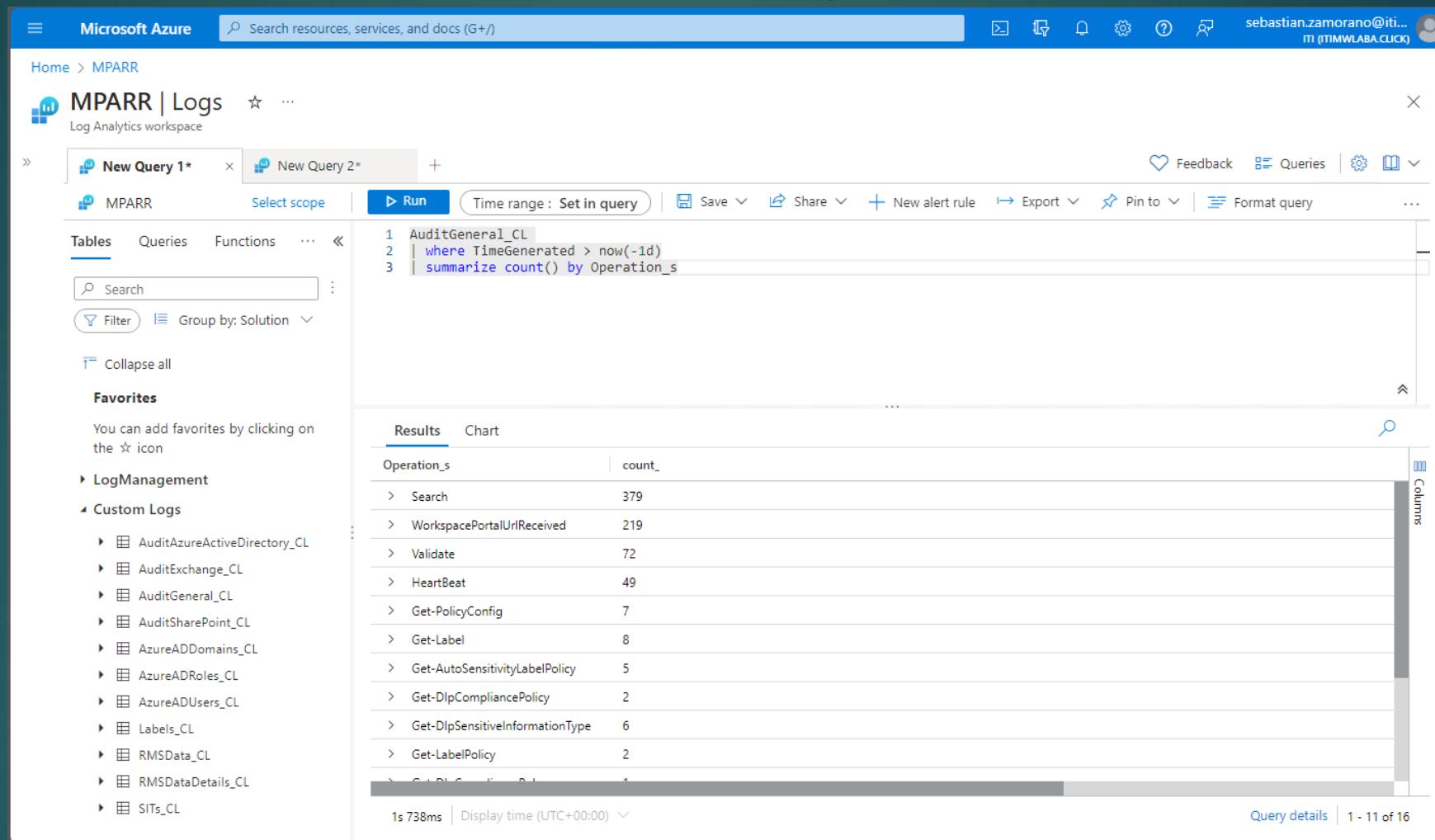
- AuditAzureActiveDirectory_CL
- AuditExchange_CL
- AuditGeneral_CL
- AuditSharePoint_CL
- AzureADDomains_CL
- AzureADRoles_CL
- AzureADUsers_CL
- Labels_CL
- RMSData_CL
- RMSDataDetails_CL
- SITs_CL

1 AuditGeneral_CL
2 | where TimeGenerated > now(-1d)
3 | summarize count() by Operation_s

Results Chart

Operation_s	count_
Search	379
WorkspacePortalUrlReceived	219
Validate	72
HeartBeat	49
Get-PolicyConfig	7
Get-Label	8
Get-AutoSensitivityLabelPolicy	5
Get-DlpCompliancePolicy	2
Get-DlpSensitiveInformationType	6
Get-LabelPolicy	2
Get-DlpCompliancePolicy	1

1s 738ms Display time (UTC+00:00) Query details 1 - 11 of 16



Logs Analytics workspace

Labels information

Microsoft Azure Search resources, services, and docs (G+) Home > MPARR sebastian.zamorano@iti... ITI (ITIMWLABA.CLICK)

MPARR | Logs Log Analytics workspace

New Query 1* New Query 2* New Query 3* Run Time range : Last 24 hours Save Share New alert rule Export Pin to Format query ...

MPARR Select scope Tables Queries Functions ...

1 Labels_CL

Search Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the star icon

LogManagement

Custom Logs

- AuditAzureActiveDirectory_CL
- AuditExchange_CL
- AuditGeneral_CL
- AuditSharePoint_CL
- AzureADDomains_CL
- AzureADRoles_CL
- AzureADUsers_CL
- Labels_CL
- RMSData_CL
- RMSDataDetails_CL
- SITs_CL

Results Chart

TimeGenerated [UTC] ↑	DisplayName_s	Name_s	Guid_g	Priority_d	ParentLabelID
9/28/2023, 12:32:07.623 PM	Anyone - without protection	Anyone	654662f4-7b09-4977-9535-967e5d32ab5e	0	
9/28/2023, 12:32:07.623 PM	Personal	Personal	6ae827ea-4cae-4451-80e5-dce561dc2c5a	1	
9/28/2023, 12:32:07.623 PM	Común	Común	b1735137-4b04-41ee-8684-178bc3e0736f	2	
9/28/2023, 12:32:07.623 PM	Public	Public	de8d1dda-3efd-4a4d-9471-27fc5453733d	3	
9/28/2023, 12:32:07.623 PM	MIP Scanner	MIP Scanner	46db5e95-461b-4cf0-a84c-1bcc27c24296	4	
9/28/2023, 12:32:07.623 PM	KD	MIP Scanner - KD	d5c78001-714f-41d9-9441-918e24e4c613	5	MIP Scann...
9/28/2023, 12:32:07.623 PM	Internal Use	Internal Use	3283d018-5e31-40eb-b545-9f6b7c135bf3	6	
9/28/2023, 12:32:07.623 PM	Students	Internal use - Students	4ef56773-6ae7-4f8c-bfb2-4cab3345142	7	Internal Us...
9/28/2023, 12:32:07.623 PM	Anyone	Internal use - Extended	bbe5651b-afc8-40be-8560-9148568a52cd	8	Internal Us...
9/28/2023, 12:32:07.623 PM	Internal	General	f4457605-d225-4b6b-a24d-306c2d52d817	9	
9/28/2023, 12:32:07.623 PM	None	None	142321-12-15-14020-0EFL-CACF71-JL45L1	10	

0s 639ms Display time (UTC+00:00) Query details 1 - 11 of 54

Logs Analytics workspace

Top 100 users from AzureADUsers_CL

Microsoft Azure Search resources, services, and docs (G+) Home > MPARR sebastian.zamorano@iti... User profile icon

MPARR | Logs

Log Analytics workspace

New Query 1* + Add query

MPARR Select scope Run Time range: Last 24 hours Save Share New alert rule Export Pin to Format query ...

Tables Queries Functions ...

1 AzureADUsers_CL
2 | top 100 by UserPrincipalName_s

Search Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the star icon

- LogManagement
- Custom Logs
 - AuditAzureActiveDirectory_CL
 - AuditExchange_CL
 - AuditGeneral_CL
 - AuditSharePoint_CL
 - AzureADDomains_CL
 - AzureADRoles_CL
 - AzureADUsers_CL
 - Labels_CL
 - RMSData_CL
 - RMSDataDetails_CL
 - SITs_CL

Results Chart

TimeGenerated [UTC]	Department_s	UserPrincipalName_s	DisplayName_s	Mail_s
9/28/2023, 12:46:40.557 PM	Financial	vini@kazdemos.org	Vinicio Dominguez-Imbert	vini@kazdemos.org
9/28/2023, 12:46:40.401 PM		userwithoutlicense@kazdemos.org	User Without Licensing	
9/28/2023, 12:46:40.619 PM		sumit.arora@kazdemos.org	Sumit Arora	
9/28/2023, 12:46:40.760 PM		sergio.londono@kazdemos.org	Sergio Londono	sergio.londono@kazdemos.org
9/28/2023, 12:44:39.857 PM	Logistics	sebastian.zamorano.adm@kazdemos.org	Sebastian Zamorano (MCS)	sebastian.zamorano.adm@kazdemos.org
9/28/2023, 12:46:40.619 PM		ravitiwari@kazdemos.org	Ravi Tiwari	ravitiwari@kazdemos.org
9/28/2023, 12:42:45.408 PM	HR	randall.boggs@kazdemos.org	Randall Boggs	randall.boggs@kazdemos.org
9/28/2023, 12:44:40.060 PM		ramon.gonzalez@kazdemos.org	Ramon Gonzalez	ramon.gonzalez@kazdemos.org
9/28/2023, 12:44:39.716 PM		pedro.barragan@kazdemos.org	Pedro Barragan	pedro.barragan@kazdemos.org
9/28/2023, 12:46:40.323 PM	Financial	mounaimem@kazdemos.org	Mounaime Mellouk	mounaimem@kazdemos.org
9/28/2023, 12:42:45.202 PM	ITS

0s 640ms | Display time (UTC+00:00) ...

Query details | 1 - 11 of 100

Export example



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

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
```

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 MSPProducts (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 .

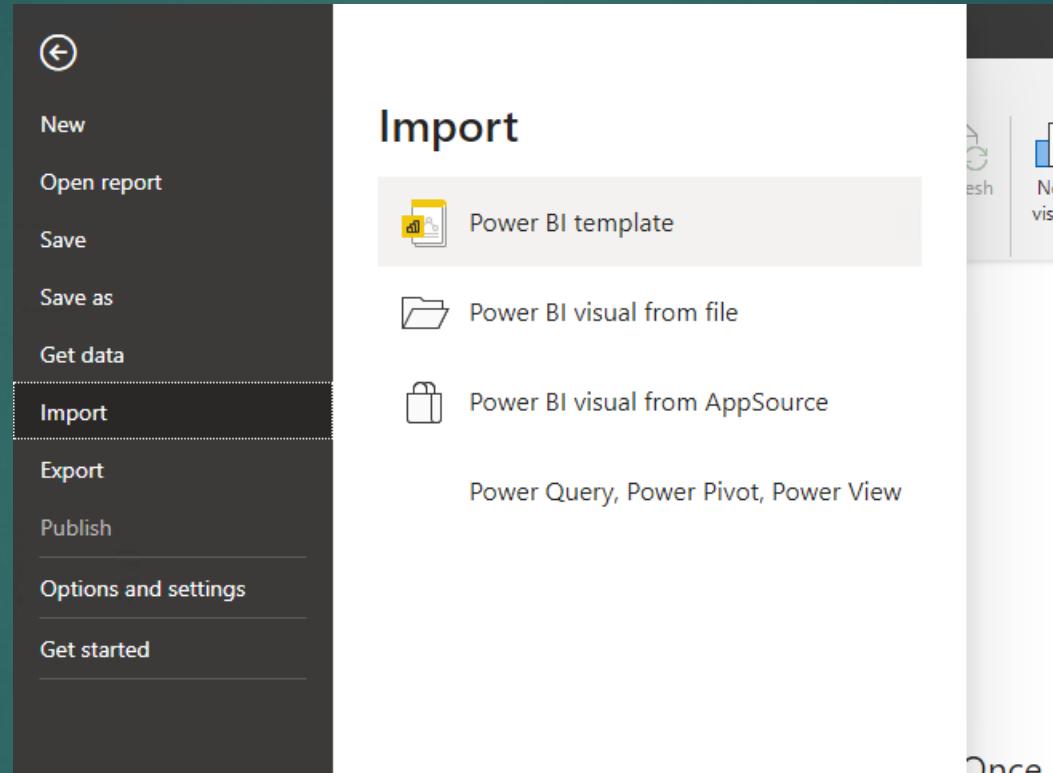


To import a Template

- ▶ 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

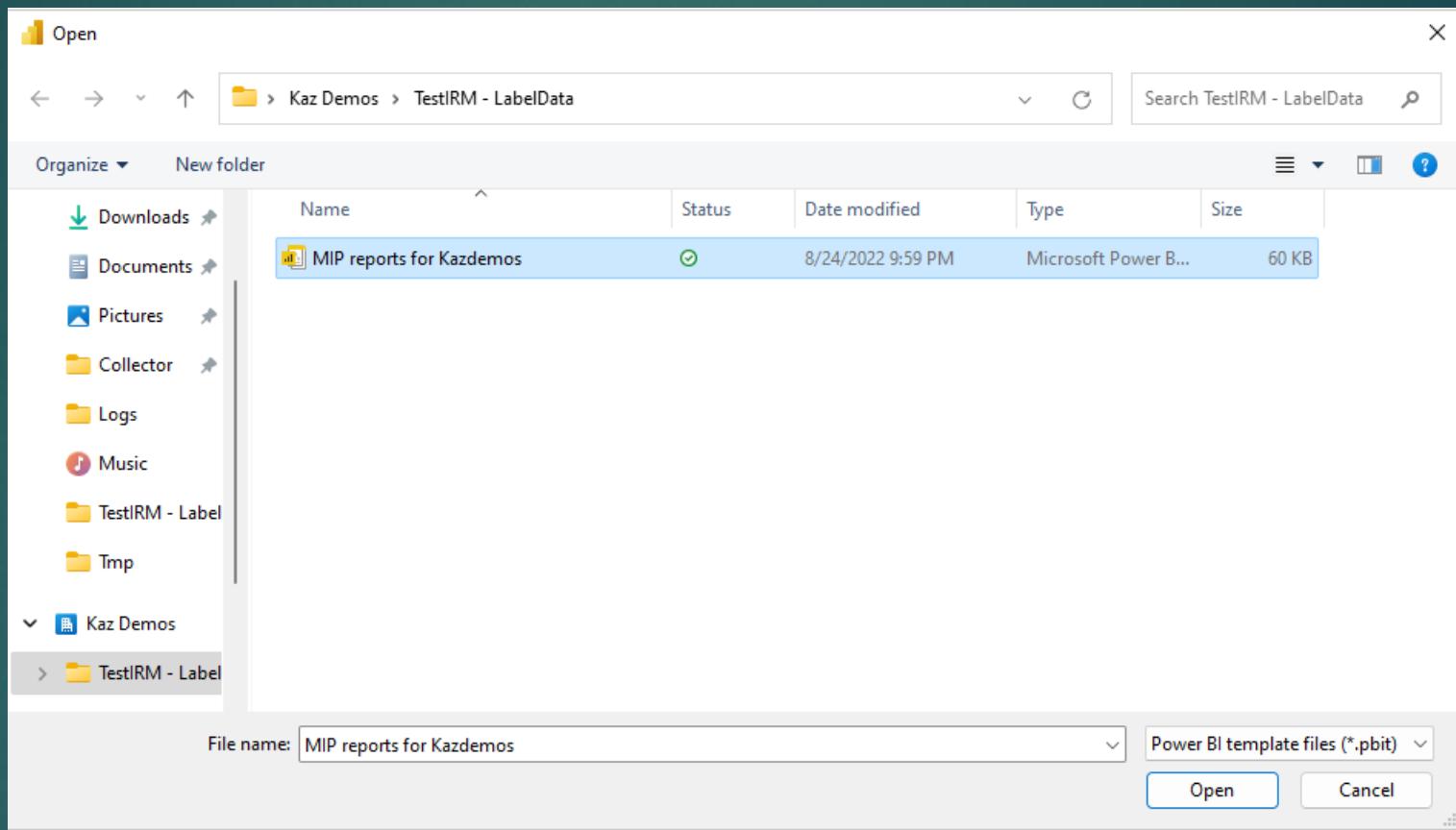
Power BI - Templates

Steps



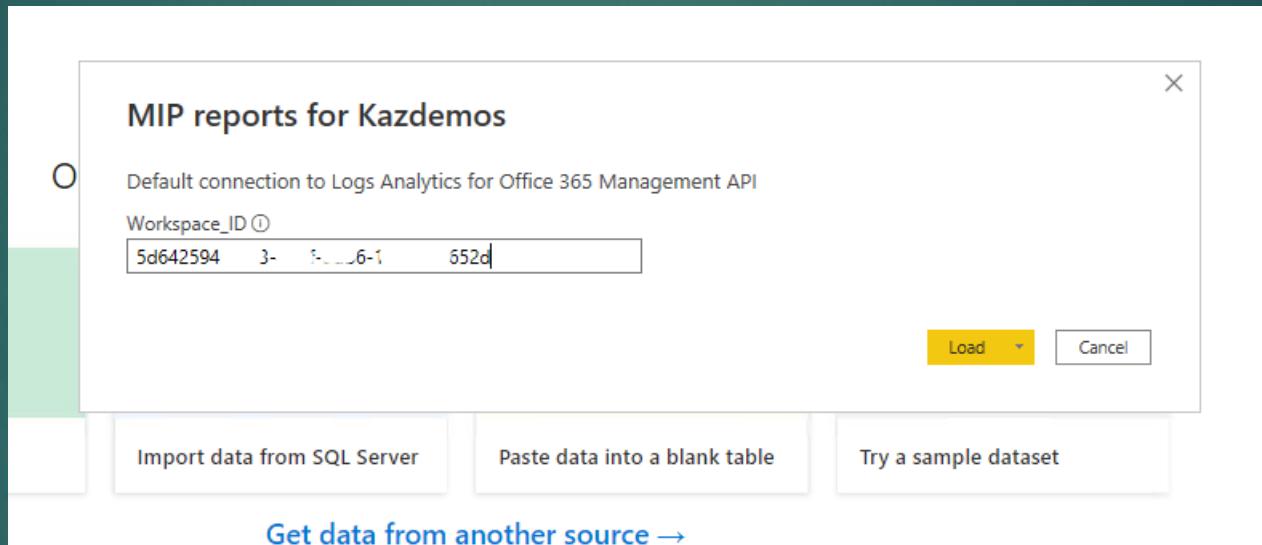
Power BI - Templates

Steps



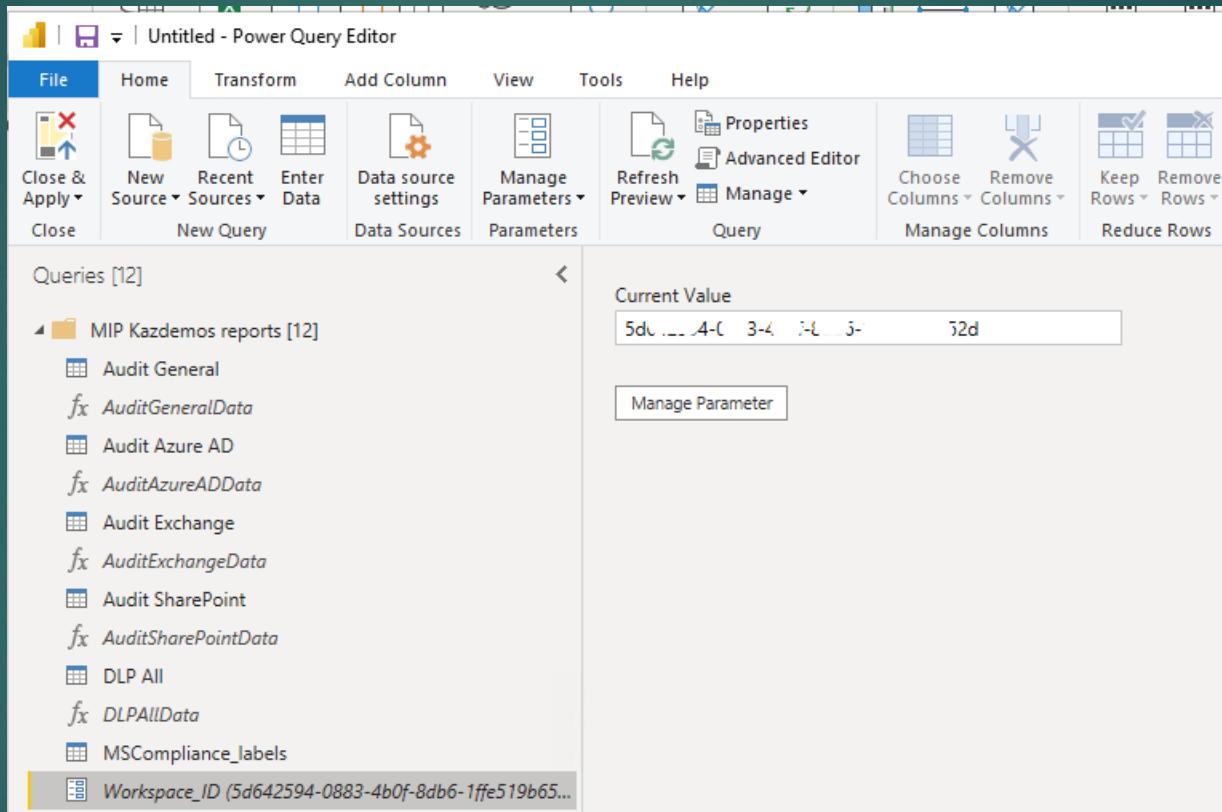
Power BI - Templates

Steps



Power BI - Templates

Steps



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>

