

# Monitor your tenant's acces with Graph and API

Andrea Martorana Tusa

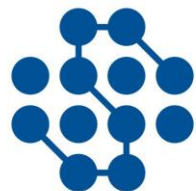


UNIVERSITÀ DEGLI STUDI DI PARMA



Bi Factory

DATA KNOWLEDGE ADVISOR



**DATA SKILLS**  
UNDERSTANDING THE WORLD



Lucient<sup>4</sup>  
ITALIA

# Speaker's info

## Andrea Martorana Tusa

- Italian living in Denmark
- Microsoft MVP Data Platform
- Product Manager in **PANDORA**
  - Admin of the Power BI tenant, Product Manager for the Content Management platform, Solution Owner for the Data and Analytics platform
- Speaker at many events worldwide
- 25+ years of experience in the world of data



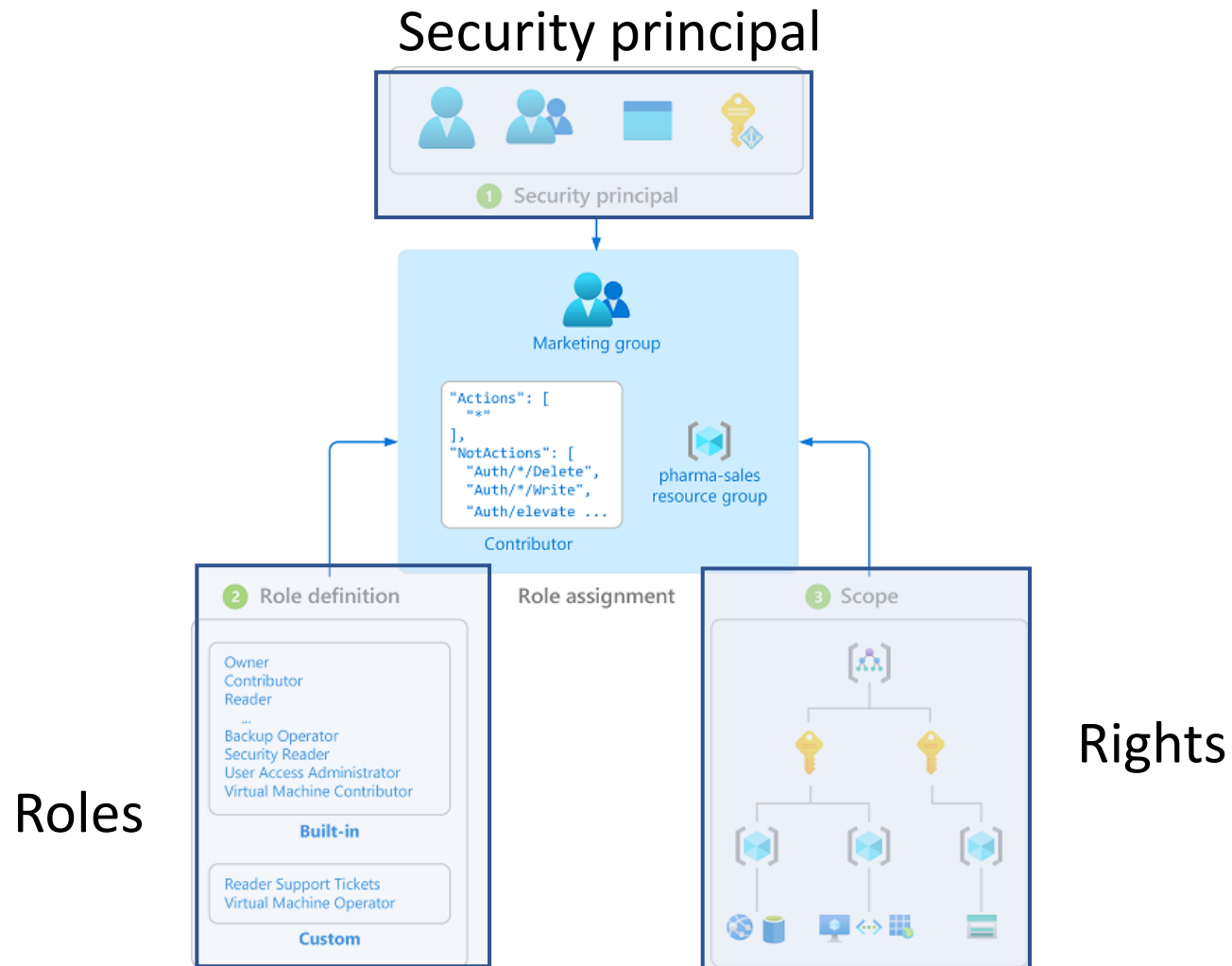
# Agenda

- Role Based Access Control
- AGDLP approach
- MS Graph API for Entra ID (Active Directory) search
- How to use the API?
- Full monitoring solution

# RBAC & AGDLP

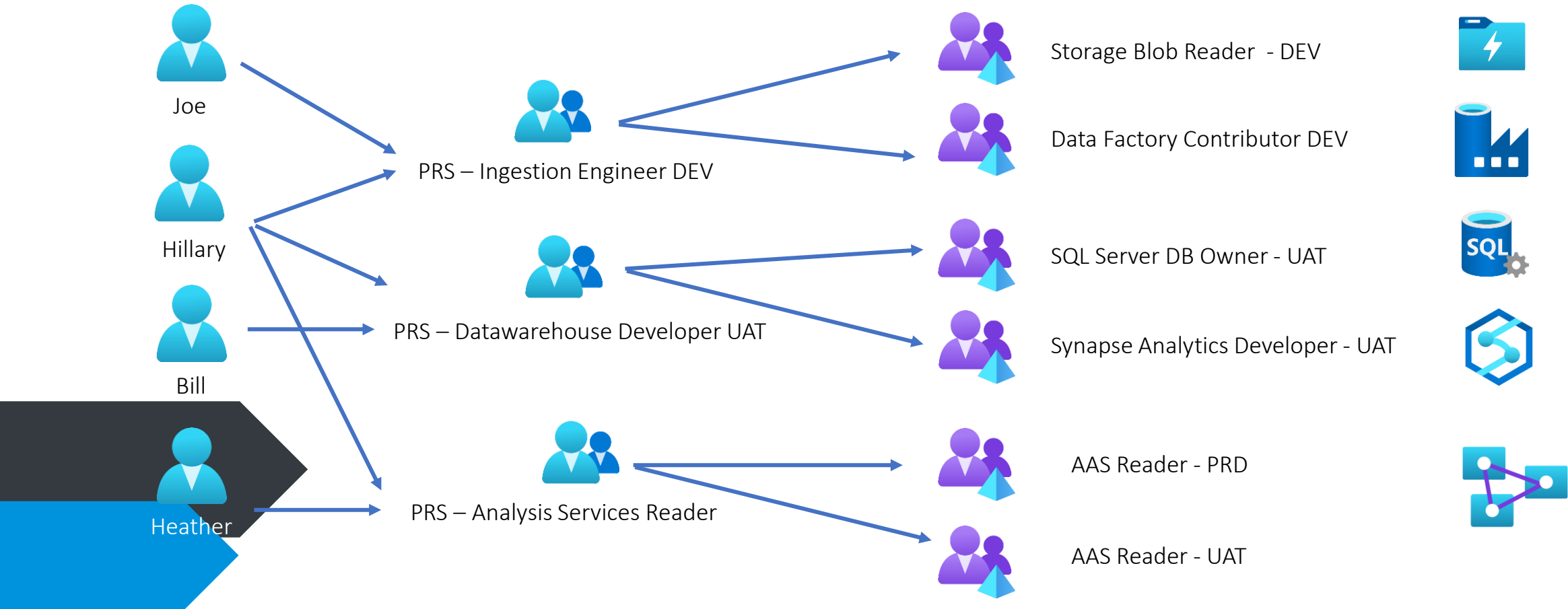


# Role-Based Access Control RBAC

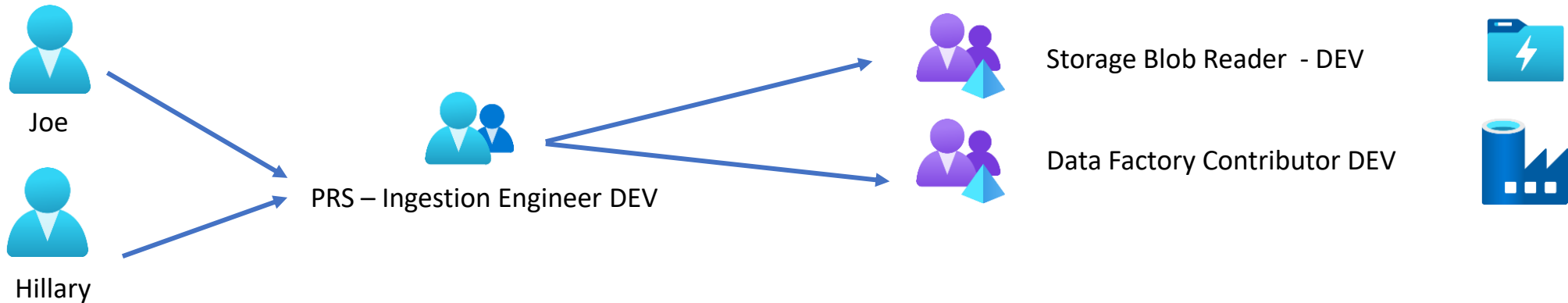


# How we implement RBAC: AGDLP architecture

A	G	DL	P
Account	Global groups (Personas)	Domain Local groups	Permission



# AGDLP architecture – key concepts



- No user account directly assigned to a resource
- All services/resources are mapped to AD Domain Local groups
- Users are assigned to Global (PRS) groups
- No user is assigned to a Domain Local group
- Domain Local groups are nested into Global groups to form a logical resources/roles grouping



# Monitor your tenant with Graph API



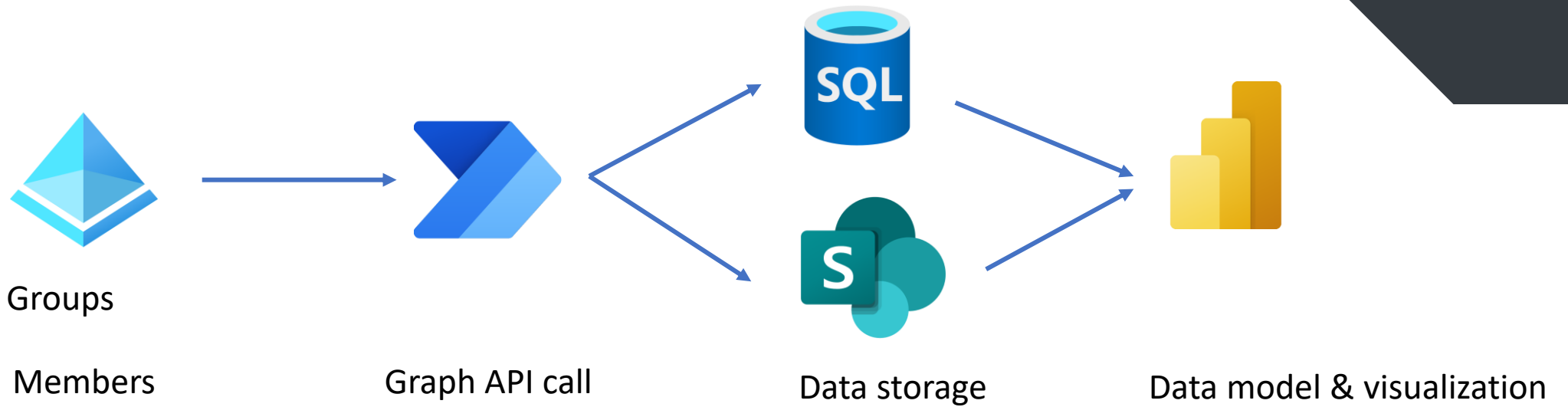
# Build an access monitoring solution

**AGDLP** security setup: **A**ccounts, **G**lobal groups, **D**omain Local groups and **P**ermissions

UserName		PersGroupName		Pers group tot members	Pers group tot member of
<div><div></div><div>Search</div></div>		<div><div></div><div>Search</div></div>		540	234
<div><div></div><div>Microsoft Entra ID</div><div>Import Data</div></div>		<div><div></div><div>SEC-AZ-EDWD-PRS-AUDIT_ADMIN</div><div>SEC-AZ-EDWD-PRS-AUDIT_DEVELOPER</div></div>			
A		G		DL	
Account		Global groups		Domain Local groups	
P				Permissions	
User ID		Persona "PRS"		Permission AD group	
UserName	PersGroupName	GroupName			
Abdusalam Bawaji	SEC-AZ-EDWZ-PRS-LOG_READER	Adm-Srv-OSWEUSQL028			
Abdusalam Bawaji	SEC-AZ-EDWZ-PRS-INGESTION_SUPPORT_L3	Adm-Srv-OSWEUSRV226			
Adam Jambori	SEC-AZ-EDWZ-PRS-INGESTION_SUPPORT_L2	Adm-Srv-OSWEUSRV227			
Adithi Angel	SEC-AZ-EDWZ-PRS-INGESTION_READER	Adm-Srv-OSWEUSRV228			
Alexandra Capina	SEC-AZ-EDWZ-PRS-INGESTION_DEVELOPER	Adm-Srv-OSWEUSRV229			
Alexander Blabanski	SEC-AZ-EDWZ-PRS-DISTRIBUTION-ANALYSIS_SERVICES_READER	SEC-ATLAS-PRD-LOG_READER			
Alexandru	SEC-AZ-EDWZ-PRS-DISTRIBUTION-ANALYSIS_SERVICES_ADMIN	SEC-AZ-EDWD-AUDIT-001-RG_Reader			
Anders Ragnvald Larsen	SEC-AZ-EDWZ-PRS-DATAWAREHOUSE_SUPPORT_L3	SEC-AZ-EDWD-AUDIT-DEV-001-Contributor			
Anthony Truong	SEC-AZ-EDWZ-PRS-DATAWAREHOUSE_SUPPORT_L2	SEC-AZ-EDWD-AUDIT-DEV-001-KV_Access			
Antoni Klenchowski	SEC-AZ-EDWZ-PRS-DATAWAREHOUSE_READER	SEC-AZ-EDWD-AUDIT-DEV-001-Reader			
Antony Marianne Ford	SEC-AZ-EDWZ-PRS-DATAWAREHOUSE_DEVELOPER	SEC-AZ-EDWD-AUDIT-DEV-001-Synapse_Admin			
Andrea Marianna Foca - admin	SEC-AZ-EDWZ-PRS-DATAWAREHOUSE_DBA	SEC-AZ-EDWD-AUDIT-DEV-001-Synapse_Contributor			
Arnel Ringe	SEC-AZ-EDWZ-PRS-AUDIT_SUPPORT_L2	SEC-AZ-EDWD-AUDIT-DEV-001-Synapse_DBOwner			
Artem Gulyaev	SEC-AZ-EDWZ-PRS-AUDIT_READER	SEC-AZ-EDWD-AUDIT-DEV-001-Synapse_PipelineExec			
Artem Trusakov	SEC-AZ-EDWZ-PRS-AUDIT_DEVELOPER	SEC-AZ-EDWD-AUDIT-DEV-001-Synapse_Reader			
Asli Karim	SEC-AZ-EDWZ-PRS-AUDIT_ADMIN	SEC-AZ-EDWD-AUDIT-SIT-001-Contributor			
Ajane Spang	SEC-AZ-EDWD-PRS-INGESTION_SUPPORT_L3	SEC-AZ-EDWD-AUDIT-SIT-001-KV_Access			
Benoit Pelt	SEC-AZ-EDWD-PRS-INGESTION_SUPPORT_L2	SEC-AZ-EDWD-AUDIT-SIT-001-Reader			
Cristina Mota	SEC-AZ-EDWD-PRS-INGESTION_READER	SEC-AZ-EDWD-AUDIT-SIT-001-Synapse_Admin			
Cristian Brindusariu	SEC-AZ-EDWD-PRS-INGESTION_DEVELOPER	SEC-AZ-EDWD-AUDIT-SIT-001-Synapse_Contributor			
Cristian Brindusariu	SEC-AZ-EDWD-PRS-DISTRIBUTION-ANALYSIS_SERVICES_READER	SEC-AZ-EDWD-AUDIT-SIT-001-Synapse_DBOwner			
Chucky Barker	SEC-AZ-EDWD-PRS-DISTRIBUTION-ANALYSIS_SERVICES_ADMIN	SEC-AZ-EDWD-AUDIT-SIT-001-Synapse_Reader			

Monitoring occurs  
via an ad hoc  
Power BI report:  
who can see what

# Workflow



# Microsoft Graph API



# Use the Microsoft Graph API



Microsoft Graph is a RESTful web API that enables you to access Microsoft Cloud service resources.

Base pattern:

```
http://graph.microsoft.com/v1.0/{resource}?[query_parameters]
```



<https://learn.microsoft.com/en-us/graph/use-the-api>

[Overview of Microsoft Graph](#)[Authentication and authorization](#)[Use the API](#)[Migrate](#)[Use SDKs](#)[Use the toolkit](#)[Resources](#)[API v1.0 reference](#)[Overview](#)[Users](#)[Groups](#)[Applications](#)[Calendars](#)[Change notifications](#)[Compliance](#)[Cross-device experiences](#)[Customer booking](#)[Device and app management](#)[Cloud printing](#)[Corporate management](#)[Service health and communications](#)[Education](#)[Extensions](#)[Files](#)[Identity and access](#)[Mail](#)[Notes](#)[People and workplace intelligence](#)[Personal contacts](#)

# Microsoft Graph REST API v1.0 endpoint reference

Article • 07/01/2022 • 2 minutes to read • 10 contributors

[Feedback](#)

Welcome to Microsoft Graph REST API reference for the v1.0 endpoint.

API sets on the v1.0 endpoint (<https://graph.microsoft.com/v1.0>) are in general availability (GA) status, and have gone through a rigorous review-and-feedback process with customers to meet practical, production needs. Updates to APIs on this endpoint are additive in nature and do not break existing app scenarios.

## Common use cases

The power of Microsoft Graph lies in easy navigation of entities and relationships across different services exposed on a single Microsoft Graph REST endpoint.

A number of these services are designed to enable rich scenarios around a [user](#) and around a [group](#).

## User-centric use cases in v1.0

1. [Get the profile](#) and [photo](#) of a user, Lisa.
2. [Get the profile information about Lisa's manager](#) and [IDs of her direct reports](#), all stored in Azure Active Directory.
3. [Access Lisa's files on OneDrive for Business](#), find the [identity](#) of the last person who modified a [file](#) there, and navigate to that person's profile.
4. [Access Lisa's calendar](#) on Exchange Online and [determine the best time for Lisa to meet with her team](#) in the next two weeks.
5. [Subscribe to](#) and [track changes](#) in Lisa's calendar, tell Lisa when she is spending more than 80% of her time in meetings.
6. [Set automatic replies](#) when Lisa is away from the office.
7. [Get the people who are most relevant to Lisa](#), based on communication, collaboration, and business relationships.
8. Get the latest sales projection from a [chart](#) in an Excel file in Lisa's OneDrive for Business.
9. [Find the tasks assigned to Lisa in Planner](#).

# Use the Microsoft Graph API

`{resource}`

- Users
- Groups
- Applications
- Calendars
- ...
- Mail
- ...
- Personal contacts
- ...

`[query_parameters]`

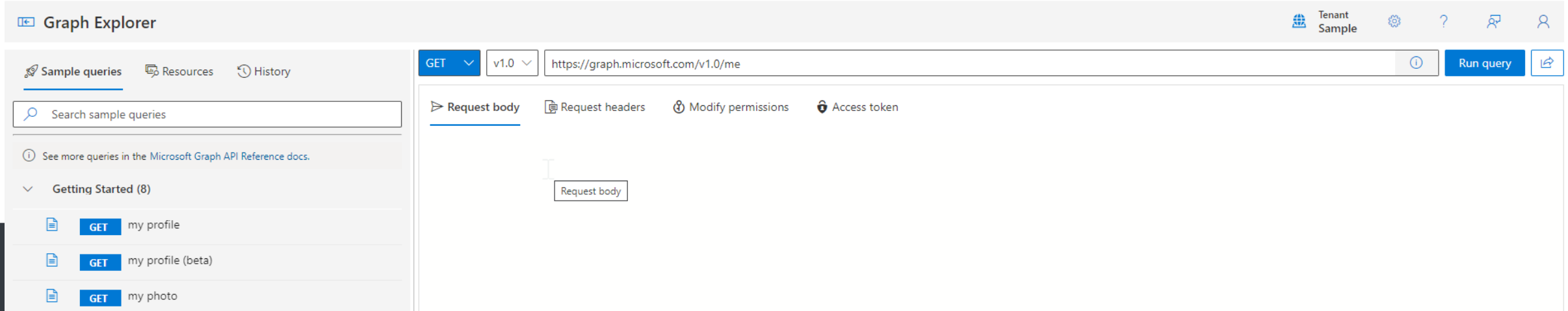
OData system query options

- Filter
- Expand
- Select
- OrderBy
- Top
- Skip
- Count
- Search
- ...

# Tools for interacting with MS Graph

## Graph Explorer

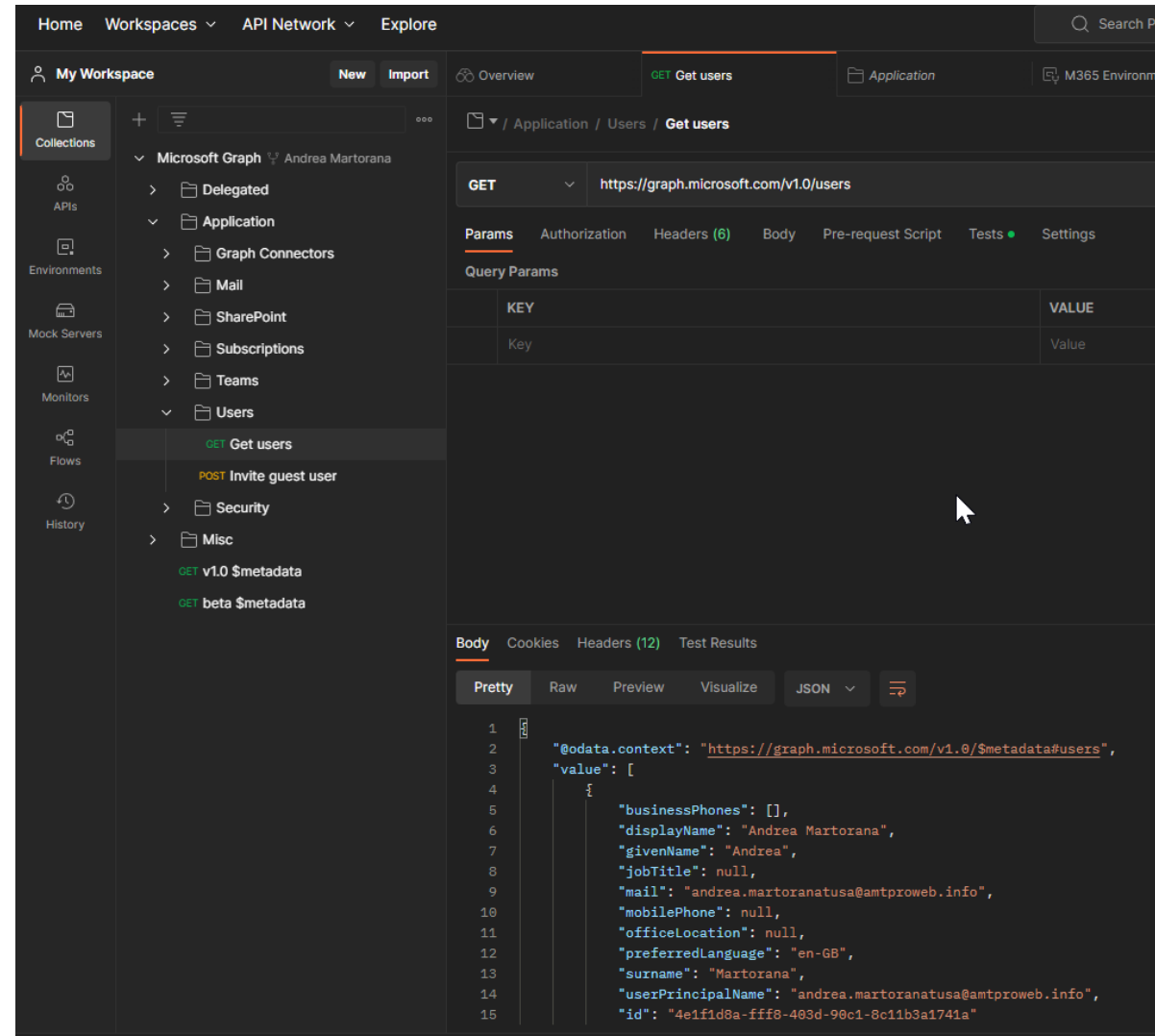
<https://developer.microsoft.com/graph/graph-explorer>.





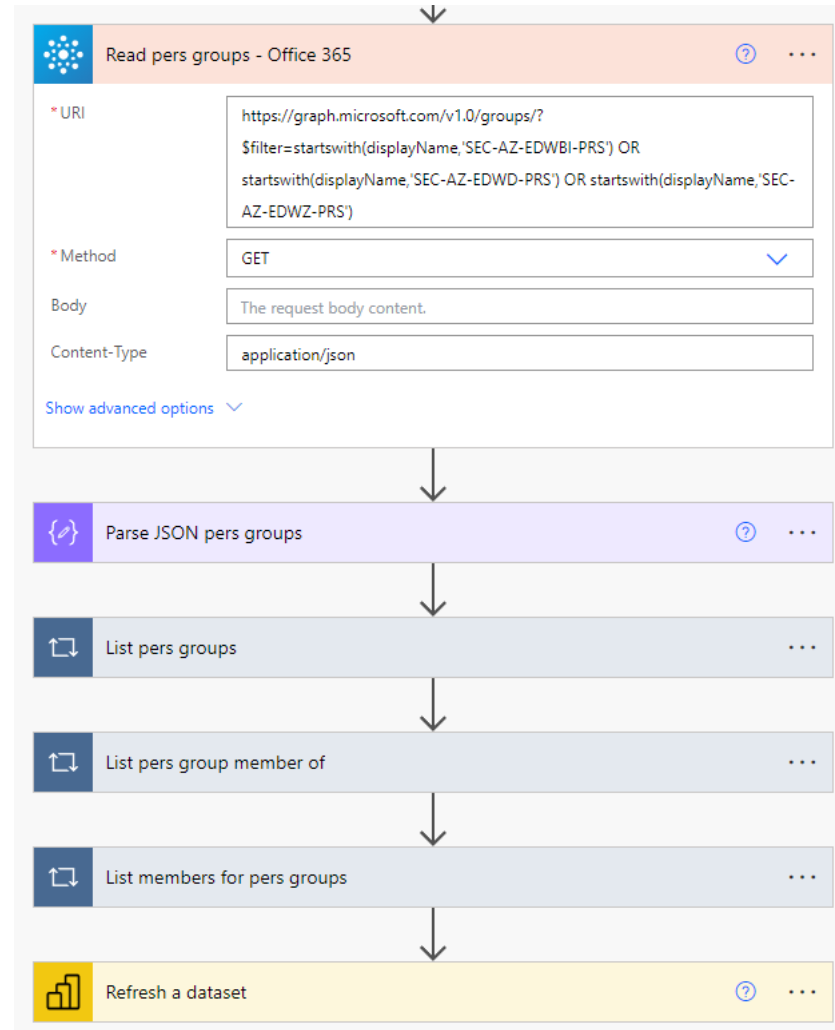
# Tools for interacting with MS Graph

Postman:



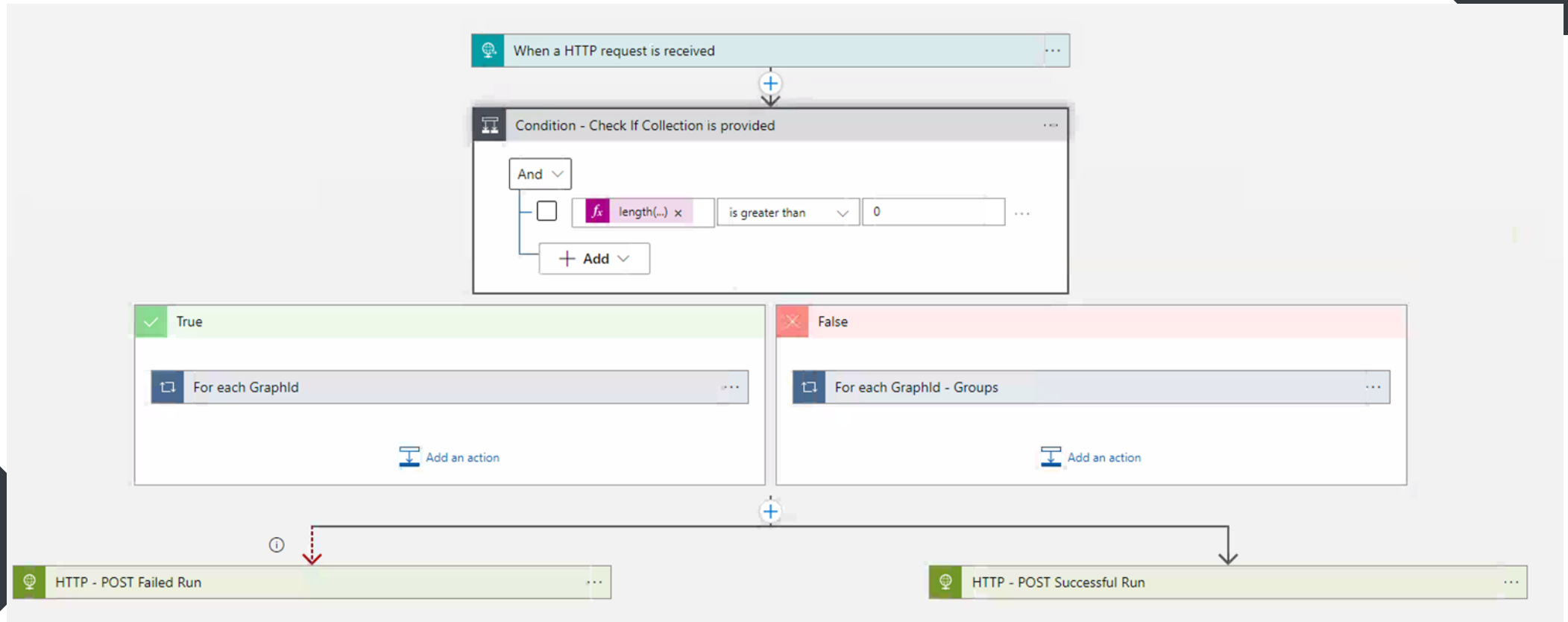
# Tools for interacting with MS Graph

## Power Automate:



# Tools for interacting with MS Graph

## Logic Apps:



# Demo

- API call with Graph Explorer
- API call with Postman



# Demo

- Build a Power Automate Flow to invoke Active Directory Graph APIs
- 
- 

# Q&A

Data Saturday #37 Feedback Form





#37 PARMA 2023

Grazie!!!



# References

- <https://learn.microsoft.com/en-us/graph/api/overview?view=graph-rest-1.0>
- <https://learn.microsoft.com/en-us/graph/use-the-api>
- <https://developer.microsoft.com/en-us/graph/graph-explorer>
- <https://learn.microsoft.com/en-us/graph/use-postman>
- <https://learn.microsoft.com/en-us/graph/traverse-the-graph>
- <https://learn.microsoft.com/en-us/azure/role-based-access-control/overview>
- <https://en.wikipedia.org/wiki/AGDLP>
- <https://www.techtarget.com/searchwindowsserver/tip/Active-Directory-nesting-groups-strategy-and-implementation>