
Identity
Insights

Agenda

- Intro
- Assumptions
- What is Identity Governance?
- Why is this hard?
- Solution roadmap
- Entra Identity Governance
- Identity Insights
- Demo

Intro

Wim van den Heijkant

Aged 39, happily married, father of two.

Full time Microsoft Identity consultant for over 15 years now.
MIIS, ILM, FIM, MIM, BPOS, Azure AD, EntraID

Co-founder and proud member of Identity Consultancy “Maatschap Fortigi”

Intro

Working with Port of Rotterdam

Cool place to work, allowed me to share, to open source:
https://github.com/fortigi/IdentityInsights

Assumptions

You have done the basics

- Automated provisioning (from HR)
- MFA, Conditional Access
- Single Sign-On & SCIM
- Just in Time Access to critical stuff
- On a path to transition from AD to EntraID

What's next… Identity Governance

What is Identity Governance?

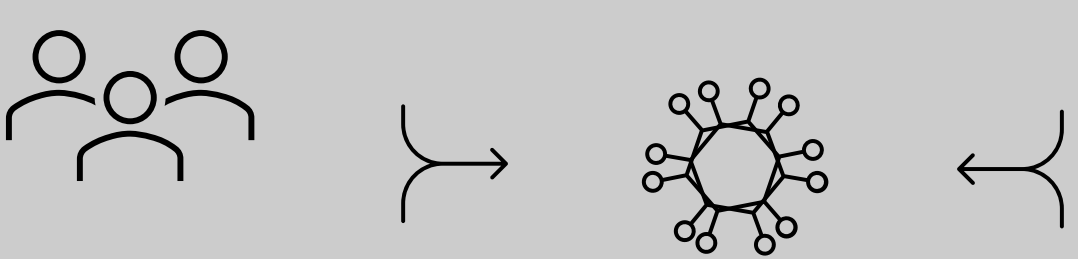
Identity **Governance** & Administration (IGA)

"Governance is the process of making and enforcing decisions"

Finding a way to "know" that the right **users** have the right **permissions** at the right time.

1) https://en.wikipedia.org/wiki/Governance

Why is this hard?

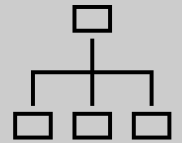


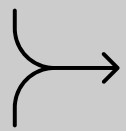
Users

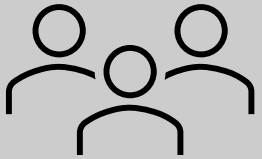
Lots of combinations

Permissions

Why is this hard?







Users

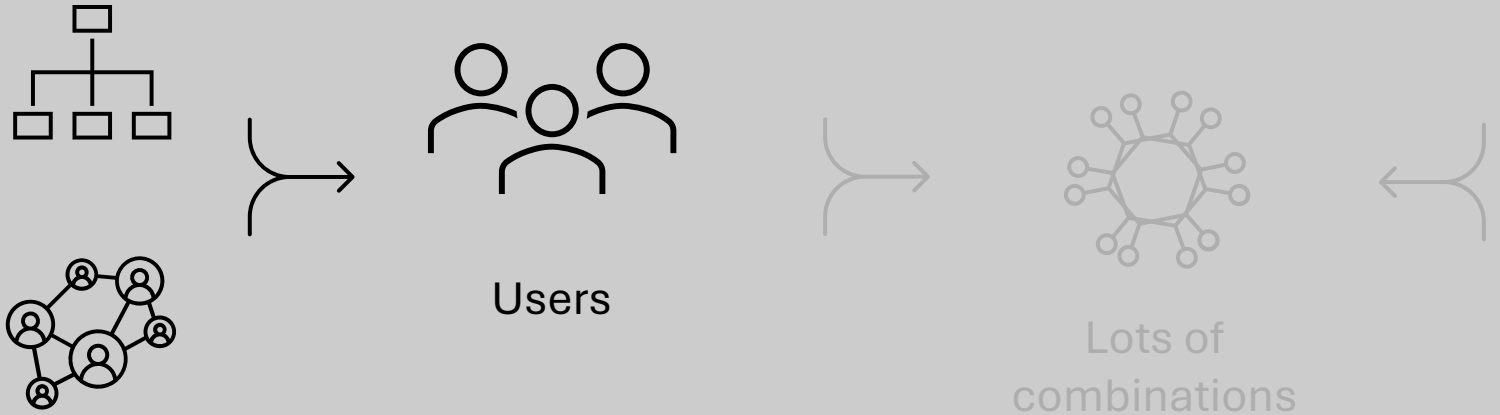
Lots of combinations

Permissions

Do you know why we have a user?

- Source of record
- Chain of responsibility
- Not easy, but we can do this!

Why is this hard?



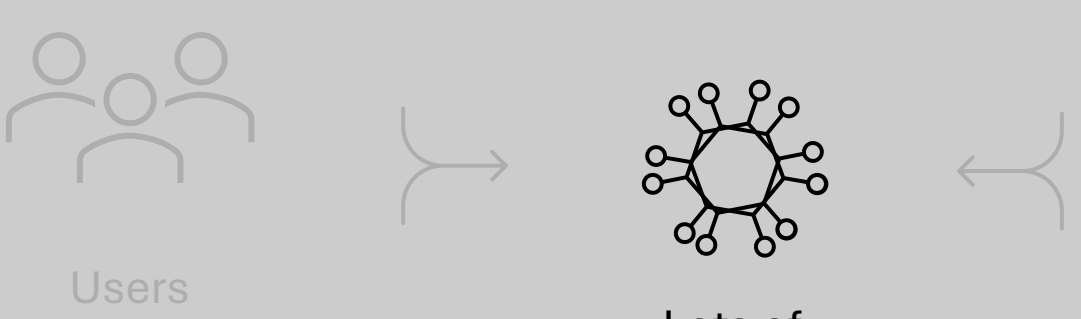
Do you know why we have a user?

- Source of record
- Chain of responsibility
- Not easy, but we can do this!

Do you know what a permission is for?

- Link to Application
- Link to team / owner
- Really hard, be we can try..

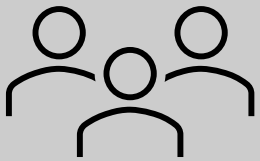
Why is this hard?



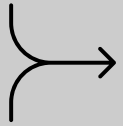
Do you know the right users have the right permissions?

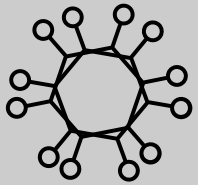
- Lots of combinations
- Lots of changes over time
- Multiple people might have an opinion

Our data...

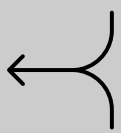


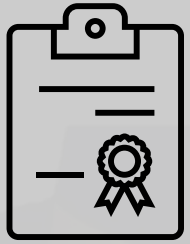
4663





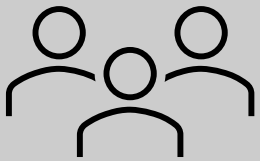
159945



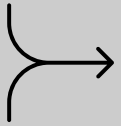


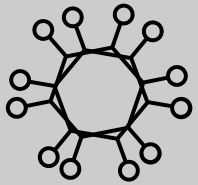
8815

Our data...

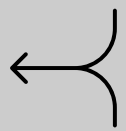


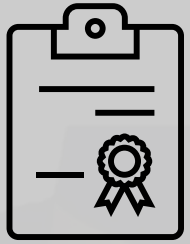
4663



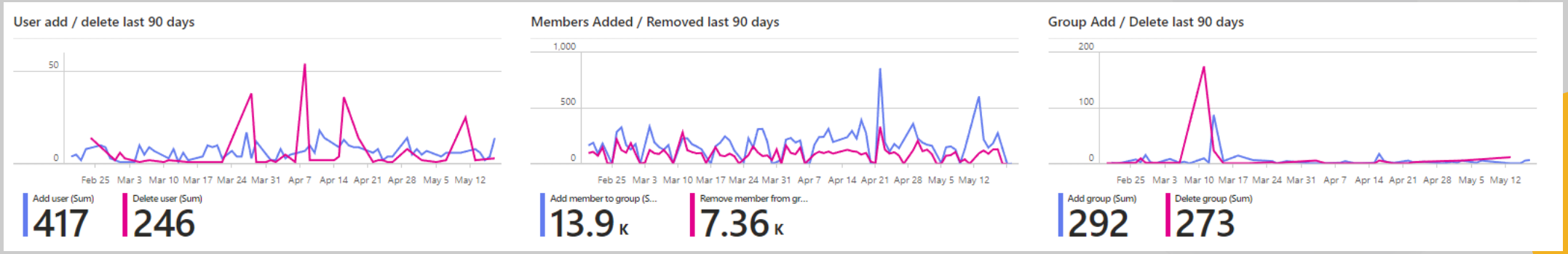


159945

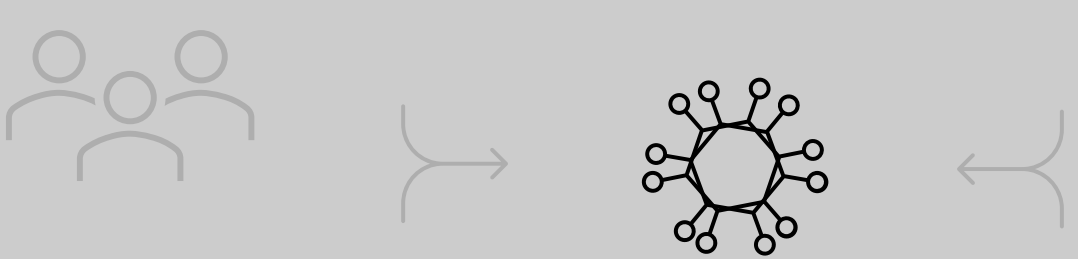




8815



As I said...



Lots of
combinations

- Lots of combinations
- Lots of changes over time

Without “help” it is impossible to know if the right users have the right permissions.

The challenge

How to “know” that the current (and future) user / permission combinations are correct.

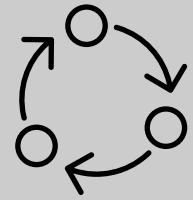
Solution roadmap

1. Start with “knowing” you have the right users
    - Source of Authority
    - Chain of responsibility

2. Proceed with “knowing” your permissions
    - Link to app
    - Link to team/owner
    - Removing (a lot) of groups

3. Next, split the user/permission combinations into parts
    - Finding clusters (‘role mining’)
    - Create roles / access packages

Entra Identity Governance



Life cycle workflows

Access Governance

- Access packages
  - Request & Approve
  - Dynamic
- Governance
  - Access Review
  - Approval logs
  - Grace periods

Entra Identity Governance

- ✓ Start with “knowing” you have the right users
  - ✓ Source of Authority
  - ✓ Chain of responsibility

- Proceed with “knowing” your permissions
  - Link to app
  - Link to team/owner
  - Removing (a lot) of groups

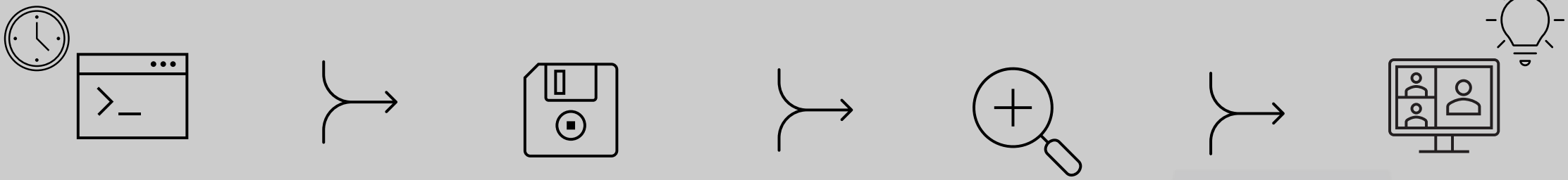
- Next, split the user/permission combinations into parts
  - Finding clusters (‘role mining’)
  - ✓ Create roles / access packages

Insights are missing..

- AI will solve all this right?
  - Well possibly… I have heard about some cool features coming..
- What did we use before AI to solve for these kinds of challenges?
  - BI….. PowerBI…
- Introducing Identity Insights


Identity
Insights

Identity Insights



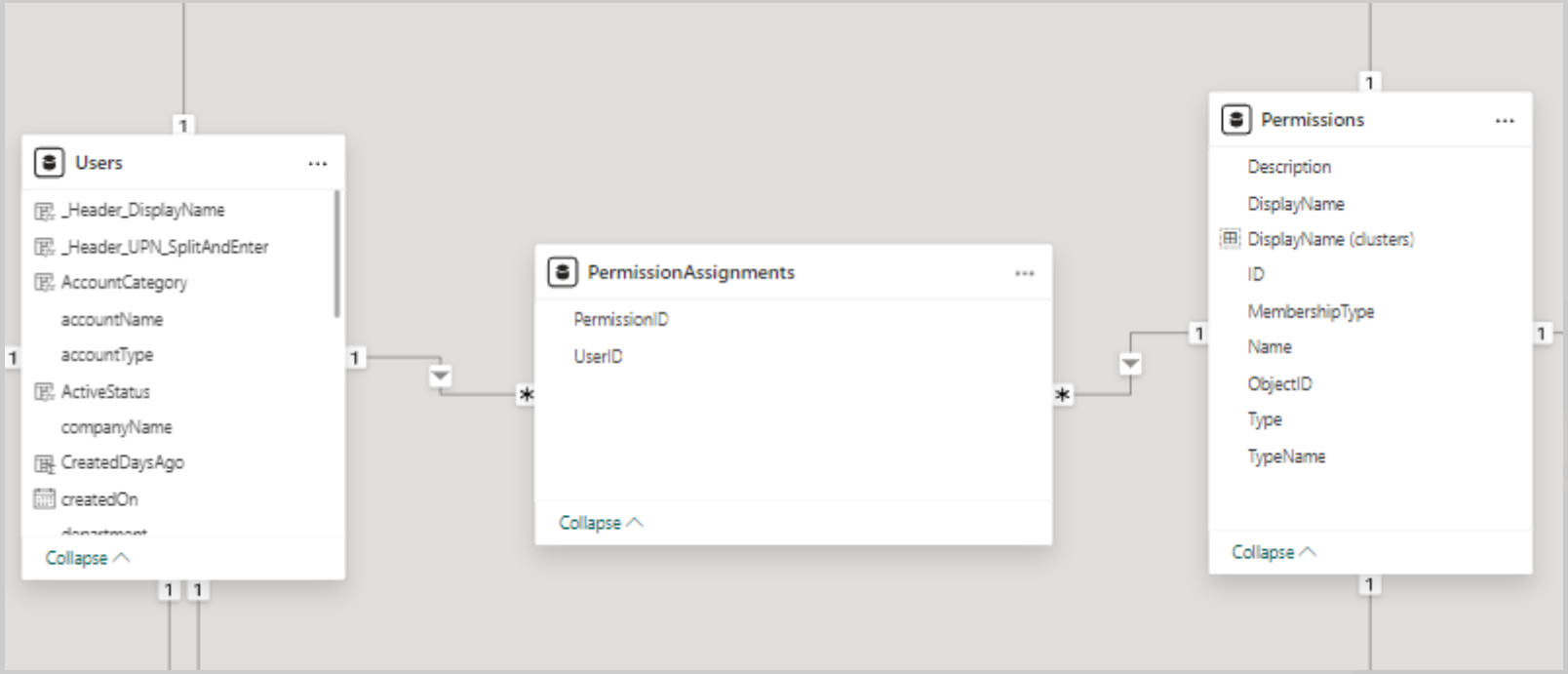
Scripts collect data
Scheduled in automation

JSON Files
Stored in Blob Storage

Joined & structured
Using Power Query

Insights using
PowerBI

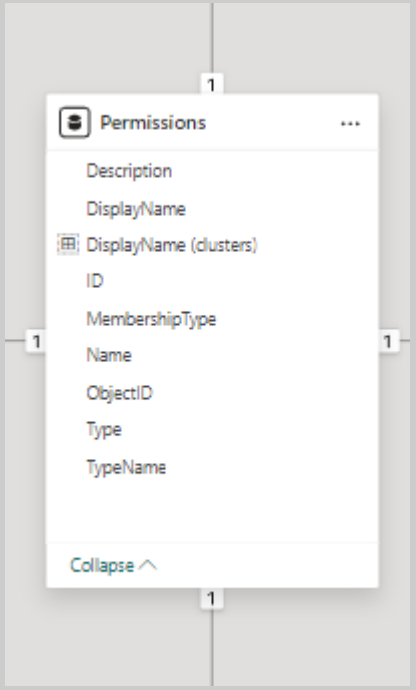
Identity Insights



Data model

There is no ID in EntraID, there is only user.

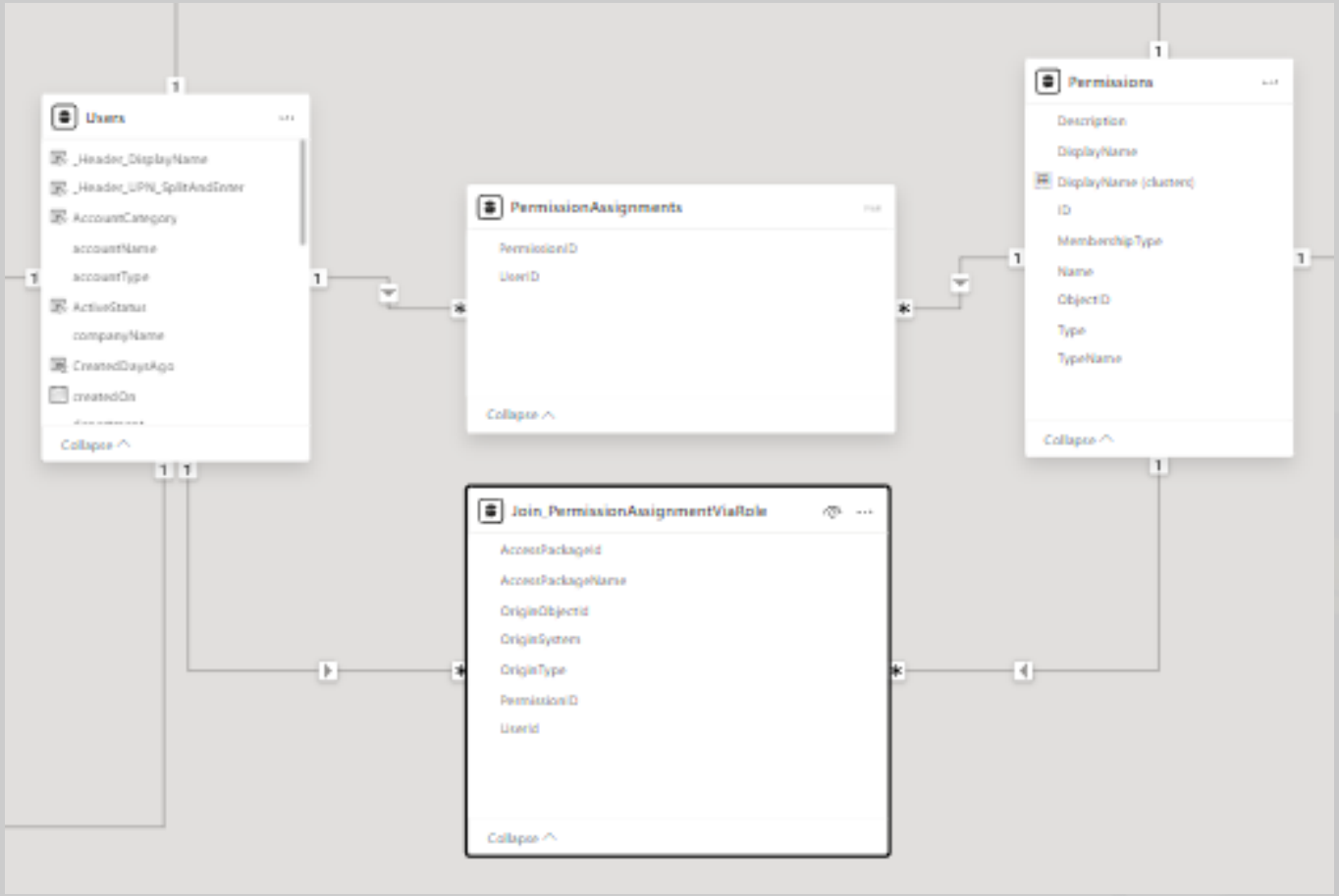
Identity Insights




```
Permissions = Union(
    selectcolumns(MSGraph_Group,
        "DisplayName", MSGraph_Group[displayName]&" (MSGraph.Group.Member)",
        "ID", "MSGraph.Group.Member|"&MSGraph_Group[id],
        "Name", MSGraph_Group[displayName],
        "ObjectID", MSGraph_Group[id],
        "Type", "MSGraph.Group.Member",
        "Description", MSGraph_Group[description],
        "TypeName", MSGraph_Group[GroupTypeName_Calc],
        "MembershipType", MSGraph_Group[MembershipType_Calc]
        ),
    selectcolumns(MSGraph_Group,
        "DisplayName", MSGraph_Group[displayName]&" (MSGraph.Group.Owner)",
        "ID", "MSGraph.Group.Owner|"&MSGraph_Group[id],
        "Name", MSGraph_Group[displayName],
        "ObjectID", MSGraph_Group[id],
        "Type", "MSGraph.Group.Owner",
        "Description", MSGraph_Group[description],
        "TypeName", MSGraph_Group[GroupTypeName_Calc],
        "MembershipType", MSGraph_Group[MembershipType_Calc]
        ),
    selectcolumns(MSGraph_Group,
        "DisplayName", MSGraph_Group[displayName]&" (MSGraph.Group.EligibleMember)",
        "ID", "MSGraph.Group.EligibleMember|"&MSGraph_Group[id],
```

Unions & Mappings make it flexible

Identity Insights



Permission Assignment via Access Package

4688
Users

161K
User / Permission Assignments

8842
Permissions

358
Access Packages

4485
User / Permission Assignments from Access Packages

271
Permissions in Access Packages

Based on Microsoft Graph data export on; 5/19/2024 11:01:56 PM

Port of Rotterdam

Role mining

Finding a sets of permissions that users matching a set of criteria have in common

Example, which permissions can we (auto) assign to;

- *all employees?*
- *all users in department y*
- *all users in department y with job title x*

This allows us to “know” for this set of user / permission combinations that they are correct.

Role mining

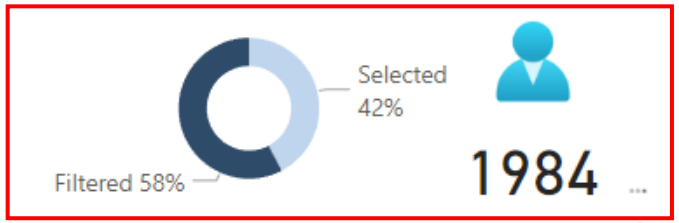
Role mining in two steps;

1. Create a “filter” selecting a sub-set of your users and/or permissions

2. Find which permissions these users have in common
    - Look at percentages (Role %)
        - % of users with permission (in this scope)
        - % of users without permission (in this scope)
        - % of users with this permission (outside of this scope)
        - % role candidate
    - Looking for patterns…

Role mining

Filter | Role % | Role X | RBAC Notes



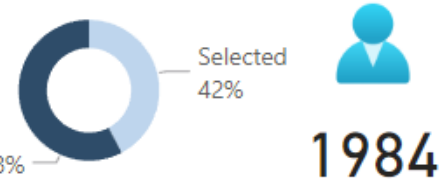
DisplayName	Description	% Role Candidate	% of Users with this Permission Assignment (In this scope)	# of Users with Permission Assignment (In this scope)	# of Users without Permission Assignment (In this Scope)	% of Users with this Permission Assignment (Outside of this scope)	# of Users with this Permission Assignment (Outside of this scope)
GG_ROL_Alle_medewerkers (MSGraph.Group.Member)		97.65	98.4	1953	31	0.79	37
_All_Users_Formeel (MSGraph.Group.Member)	Afdeling: POR\CEA\CC | 1e eigenaar BWF.Jacobs@portofrotterdam.com | 2e eigenaar: jr.gevers@portofrotterdam.com	96.93	98.5	1954	30	1.56	73
GG_APL_O365_E5-Default (MSGraph.Group.Member)	Office 365 Enterprise E5 - Customer specific selection + EMS	95.06	97.0	1924	60	1.92	90
GG_ServiceNow-dev-CHG0005693 (MSGraph.Group.Member)	Betreft user provisioning op de service now dev omgeving	93.76	98.1	1947	37	4.37	205
GG_APP_ServiceNow_Allusers_P (MSGraph.Group.Member)	CHG0005693, members worden via een script gevuld en hebben toegang to ServiceNow	88.69	98.4	1953	31	9.75	457

Users in Filter: 1984

Role mining

Filter | Role % | Role X

RBAC Notes



DisplayName	Description	% Role Candidate	% of Users with this Permission Assignment (In this scope)	# of Users with Permission Assignment (In this scope)	# of Users without Permission Assignment (In this Scope)	% of Users with this Permission Assignment (Outside of this scope)	# of Users with this Permission Assignment (Outside of this scope)
GG_ROL_Alle_medewerkers (MSGraph.Group.Member)		97.65	98.4	1953	31	0.79	37
_All_Users_Formeel (MSGraph.Group.Member)	Afdeling: POR\CEA\CC | 1e eigenaar BWF.Jacobs@portofrotterdam.com | 2e eigenaar: jr.gevers@portofrotterdam.com	96.93	98.5	1954	30	1.56	73
GG_APL_O365_E5-Default (MSGraph.Group.Member)	Office 365 Enterprise E5 - Customer specific selection + EMS	95.06	97.0	1924	60	1.92	90
GG_ServiceNow-dev-CHG0005693 (MSGraph.Group.Member)	Betreft user provisioning op de service now dev omgeving	93.76	98.1	1947	37	4.37	205
GG_APP_ServiceNow_Allusers_P (MSGraph.Group.Member)	CHG0005693, members worden via een script gevuld en hebben toegang to ServiceNow	88.69	98.4	1953	31	9.75	457

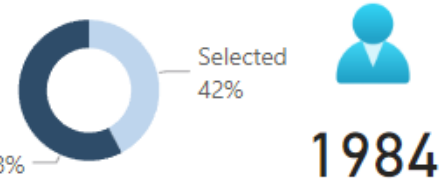
Users in Filter: 1984

98,4% of user in filter have this permission (Total **1953**)
31 do not.. Would get this permission if auto assigned

Role mining

Filter | Role % | Role X

RBAC Notes



DisplayName	Description	% Role Candidate	% of Users with this Permission Assignment (In this scope)	# of Users with Permission Assignment (In this scope)	# of Users without Permission Assignment (In this Scope)	% of Users with this Permission Assignment (Outside of this scope)	# of Users with this Permission Assignment (Outside of this scope)
GG_ROL_Alle_medewerkers (MSGraph.Group.Member)		97.65	98.4	1953	31	0.79	37
_All_Users_Formeel (MSGraph.Group.Member)	Afdeling: POR\CEA\CC | 1e eigenaar BWF.Jacobs@portofrotterdam.com | 2e eigenaar: jr.gevers@portofrotterdam.com	96.93	98.5	1954	30	1.56	75
GG_APL_O365_E5-Default (MSGraph.Group.Member)	Office 365 Enterprise E5 - Customer specific selection + EMS	95.06	97.0	1924	60	1.92	90
GG_ServiceNow-dev-CHG0005693 (MSGraph.Group.Member)	Betreft user provisioning op de service now dev omgeving	93.76	98.1	1947	37	4.37	205
GG_APP_ServiceNow_Allusers_P (MSGraph.Group.Member)	CHG0005693, members worden via een script gevuld en hebben toegang to ServiceNow	88.69	98.4	1953	31	9.75	457

Users in Filter: 1984

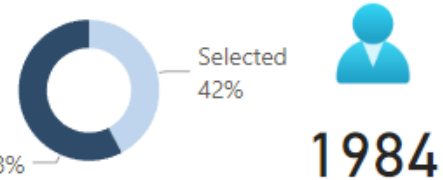
98,4% of user in filter have this permission (Total **1953**)
31 do not.. Would get this permission if auto assigned

37 users have this permission but are not in the filter.

Role mining

Filter | Role % | Role X

RBAC Notes



DisplayName	Description	% Role Candidate	% of Users with this Permission Assignment (In this scope)	# of Users with Permission Assignment (In this scope)	# of Users without Permission Assignment (In this Scope)	% of Users with this Permission Assignment (Outside of this scope)	# of Users with this Permission Assignment (Outside of this scope)
GG_ROL_Alle_medewerkers (MSGraph.Group.Member)		97.65	98.4	1953	31	0.79	37
_All_Users_Formeel (MSGraph.Group.Member)	Afdeling: POR\CEA\CC | 1e eigenaar BWF.Jacobs@portofrotterdam.com | 2e eigenaar: jr.gevers@portofrotterdam.com	96.93	98.5	1954	30	1.56	73
GG_APL_O365_E5-Default (MSGraph.Group.Member)	Office 365 Enterprise E5 - Customer specific selection + EMS	95.06	97.0	1924	60	1.92	90
GG_ServiceNow-dev-CHG0005693 (MSGraph.Group.Member)	Betreft user provisioning op de service now dev omgeving	93.76	98.1	1947	37	4.37	205
GG_APP_ServiceNow_Allusers_P (MSGraph.Group.Member)	CHG0005693, members worden via een script gevuld en hebben toegang to ServiceNow	88.69	98.4	1953	31	9.75	457

% Role candidate 97,65

Role mining

Filter | Role % | Role X

RBAC Notes

Filtered
100%

22

DisplayName	Baden, Kathy	Burger, Ingrid	Fani - Alrayess, Rabia	Haandel, Betty van	Hanssen, Patricia	Heemskerk, Mariska	Item, Cees van	Kemp, Merel	Kootstra, Anne	Laure, Henk de	Leenaarts, Leon	Patty, Claus	Poel, Ton van der	Scheepbouwer, Rob	Schouwen, Mark van	Tas, Erik	Toren Jeroer
GG_APP_PaloAlto_GlobalProtect (MSGraph.Group.Member)																	
GG_APP_TemplafyDesktop (MSGraph.Group.Member)																	
GG_ORG_ROL_INK_Algemeen_EU (MSGraph.Group.Member)																	
G-OG-POR (MSGraph.Group.Member)																	
TS-Service Center Facilitair (MSGraph.Group.Member)																	
_Medwerkers_Intern (MSGraph.Group.Member)																	
GG_APP_Scinaptic_OnePlaceMail (MSGraph.Group.Member)																	
E-Learning Bedrijfscode (MSGraph.Group.Member)																	
GG_App_DominikReichl_KeepassPasswordSafe (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN D04 (EDOCS - D04) (MSGraph.Group.Member)																	
GG_APP_PDFForge_PDFCreator (MSGraph.Group.Member)																	
GG_APP_SapGUI (MSGraph.Group.Member)																	
GG_APP_SAPGUIXML (MSGraph.Group.Member)																	
GG_ROL_Facilitiy_Services (MSGraph.Group.Member)																	
GG_ROL_Facilities_Facilitaire_Dienstverlening_Intern (MSGraph.Group.Member)																	
_All Users informeel (MSGraph.Group.Member)																	
GG_APP_SAP_GUI (MSGraph.Group.Member)																	
GG_ROL_Facilitiy_Services_Intern (MSGraph.Group.Member)																	
AG_ROL_DMS_BEVEILIGING LOCATIES LEDEN (BEVEILIGEN LOCATIES) (MSGraph.Group.Member)																	
AG_ROL_DMS_FAC (OVERGEHEVELDE DOCUMENTEN UIT EDOCS) (MSGraph.Group.Member)																	
AG_ROL_DMS_FACILITIES - VERGADERINGEN LEDEN (MSGraph.Group.Member)																	
AG_ROL_DMS_HET ONDERHOUDEN VAN GEBOUWEN EN VOORZIENINGEN LEDEN (GEBOUWEN EN VOORZIENINGEN ONDERHOUDEN) (MSGraph.Group.Member)																	
AG_ROL_DMS_OPSTELLEN EN BEHEREN VAN SLAS LEDEN (SLA'S OPSTELLEN EN BEHEREN) (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN AMBULANCEVERVOER-MAASVLAKTE-2-BEHEREN (AMBULANCEVERVOER MAASVLAKTE 2 BEHEREN) (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN ARCHIEFBESCHEIDEN-OVERBRENGEN-EN-VERNIETIGEN																	

Role mining

Filter | Role % | Role X

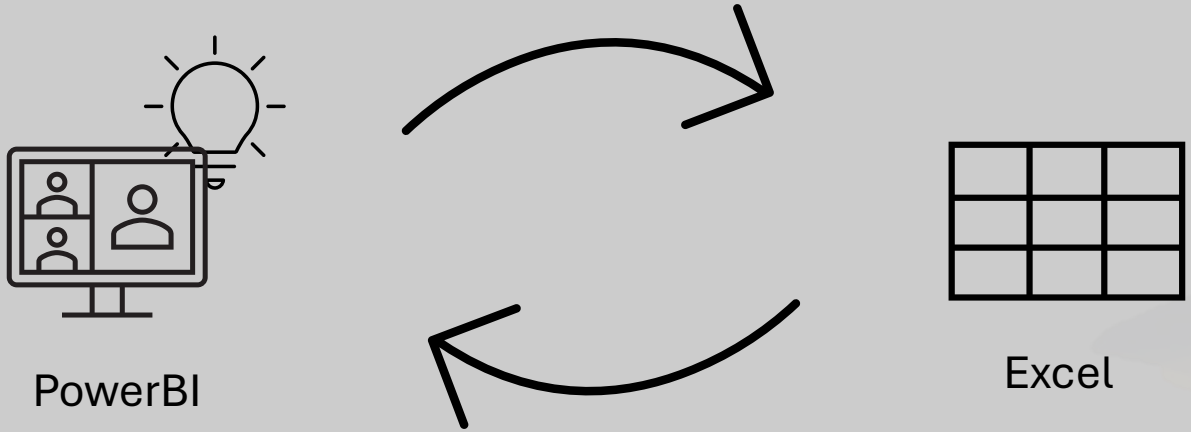
RBAC Notes

Filtered
100%

22

DisplayName	Baden, Kathy	Burger, Ingrid	Fani - Alrayess, Rabia	Haandel, Betty van	Hanssen, Patricia	Heemskerk, Mariska	Item, Cees van	Kemp, Merel	Kootstra, Anne	Laure, Henk de	Leenaarts, Leon	Patty, Claus	Poel, Ton van der	Scheepbouwer, Rob	Schouwen, Mark van	Tas, Erik	Toren Jeroer
GG_APP_PaloAlto_GlobalProtect (MSGraph.Group.Member)																	
GG_APP_TemplafyDesktop (MSGraph.Group.Member)																	
GG_ORG_ROL_INK_Algemeen_EU (MSGraph.Group.Member)																	
G-OG-POR (MSGraph.Group.Member)																	
TS-Service Center Facilitair (MSGraph.Group.Member)																	
_Medwerkers_Intern (MSGraph.Group.Member)																	
GG_APP_Scinaptic_OnePlaceMail (MSGraph.Group.Member)																	
E-Learning Bedrijfscode (MSGraph.Group.Member)																	
GG_App_DominikReichl_KeepassPasswordSafe (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN D04 (EDOCS - D04) (MSGraph.Group.Member)																	
GG_APP_PDFForge_PDFCreator (MSGraph.Group.Member)																	
GG_APP_SapGUI (MSGraph.Group.Member)																	
GG_APP_SAPGUIXML (MSGraph.Group.Member)																	
GG_ROL_Facilitiy_Services (MSGraph.Group.Member)																	
GG_ROL_Facilities_Facilitaire_Dienstverlening_Intern (MSGraph.Group.Member)																	
_All Users informeel (MSGraph.Group.Member)																	
GG_APP_SAP_GUI (MSGraph.Group.Member)																	
GG_ROL_Facilitiy_Services_Intern (MSGraph.Group.Member)																	
AG_ROL_DMS_BEVEILIGING LOCATIES LEDEN (BEVEILIGEN LOCATIES) (MSGraph.Group.Member)																	
AG_ROL_DMS_FAC (OVERGEHEVELDE DOCUMENTEN UIT EDOCS) (MSGraph.Group.Member)																	
AG_ROL_DMS_FACILITIES - VERGADERINGEN LEDEN (MSGraph.Group.Member)																	
AG_ROL_DMS_HET ONDERHOUDEN VAN GEBOUWEN EN VOORZIENINGEN LEDEN (GEBOUWEN EN VOORZIENINGEN ONDERHOUDEN) (MSGraph.Group.Member)																	
AG_ROL_DMS_OPSTELLEN EN BEHEREN VAN SLAS LEDEN (SLA'S OPSTELLEN EN BEHEREN) (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN AMBULANCEVERVOER-MAASVLAKTE-2-BEHEREN (AMBULANCEVERVOER MAASVLAKTE 2 BEHEREN) (MSGraph.Group.Member)																	
AG_ROL_RMA_BEZOEKERS VAN ARCHIEFBESCHEIDEN-OVERBRENGEN-EN-VERNIETIGEN																	

Filter noise.. Add notes



Adding notes to your Power BI data

Filtered 58%

1984

DisplayName	Description	% Role Candidate	% of Users with this Permission Assignment (In this scope)	# of Users with Permission Assignment (In this scope)	# of Users without Permission Assignment (In this Scope)	% of Users with this Permission Assignment (Outside of this scope)	# of Users with this Permission Assignment (Outside of this scope)
GG_ROL_Alle_medewerkers (MSGraph.Group.Member)		97.65	98.4	1953	31	0.79	37
_All_Users_Formeel (MSGraph.Group.Member)	Afdeling: POR\CEA\CC | 1e eigenaar BWF.Jacobs@portofrotterdam.com | 2e eigenaar: jr.gevers@portofrotterdam.com	96.93	98.5	1954	30	1.56	73
GG_APL_O365_E5-Default (MSGraph.Group.Member)	Office 365 Enterprise E5 - Customer specific selection + EMS	95.06	97.0	1924	60	1.92	90
[redacted]	[redacted]	[redacted]	98.1	1947	37	4.37	205
GG_ROL_OGD_CMDDeny (MSGraph.Group.Member)	Rolgroep met alle personen die in OurWorkplace mogen, exclusief de groep GG_ROL_OGD_CMDAllow. Wordt automatisch geüpdate via de dwp-p-awe-aut01 taskscheduler	89.20	90.9	1804	180	1.73	81
GG_ROL_OGD_RegeditDeny (MSGraph.Group.Member)	Rolgroep met alle personen die in OurWorkplace mogen, exclusief de groep GG_ROL_OGD_RegeditAllow. Wordt automatisch geüpdate via de dwp-p-awe-aut01 taskscheduler	89.19	91.0	1805	179	1.79	84
GG_APP_ServiceNow_Allusers_P (MSGraph.Group.Member)	CHG0005695, members worden via een script gevuld en hebben toegang to ServiceNow,	88.69	98.4	1953	31	9.75	457
GG_ROL_Alle_medewerkers_Intern (MSGraph.Group.Member)		70.41	70.9	1407	577	0.51	24
OGD_Intune_iOS_Users (MSGraph.Group.Member)	Deze groep bevat alle gebruikers welke gebruik maken van de OGD policies	69.46	69.6	1381	603	0.15	7

RBAC Notes

	A	B	C
1	PermissionName	PermissionID	Exclude
2	GG_ROL_OGD_RegeditDeny (MSGraph.Group.Member)	MSGraph.Group.Member|9401b669-49de-4860-9728-2362dc077373	TRUE
3	GG_ROL_OGD_CMDDeny (MSGraph.Group.Member)	MSGraph.Group.Member|8f0f625b-ca00-43d9-a47f-ec843e82046a	TRUE

Permissions Notes

Exclude

All

- [x] Select all
- [x] (Blank)
- [ ] True

Level

All

OwnedBy

All

Demo

https://github.com/fortigi/IdentityInsights


Identity
Insights