SparebankenVest

IMPLEMENT PIM ON AZURE RESOURCES

MVP

Olav Tvedt

Cloud Dude, Sparebanken Vest

Azure «roughly» speaking

Without thinking functionality

- Objects
  - Managment Groups
  - Subscriptons
  - Resource Groups
  - Resources

- Access = Roles
  - Owner
  - Contributor
  - Reader
  - + 335 other pre-defined roles
  - + Custom roles

Trivia: What is the difference between Owner og Contributor?

Agenda

- Why
- Discovery
- Cleanup
- Modify
- Apply
- Common misunderstandings and problems

Why?

Why?

- Prevent unauthorized persons from using privileged roles
- Prevent scripts from abusing escalated permissions
- Prevent mishaps from users/scripts
- Time limited access
- Monitoring

Why?

- Require approval if desired
- Require MFA token to enable roles
- Document reason for activating
- Activation notifications
  - Owner
  - The user

Active access before PIM:

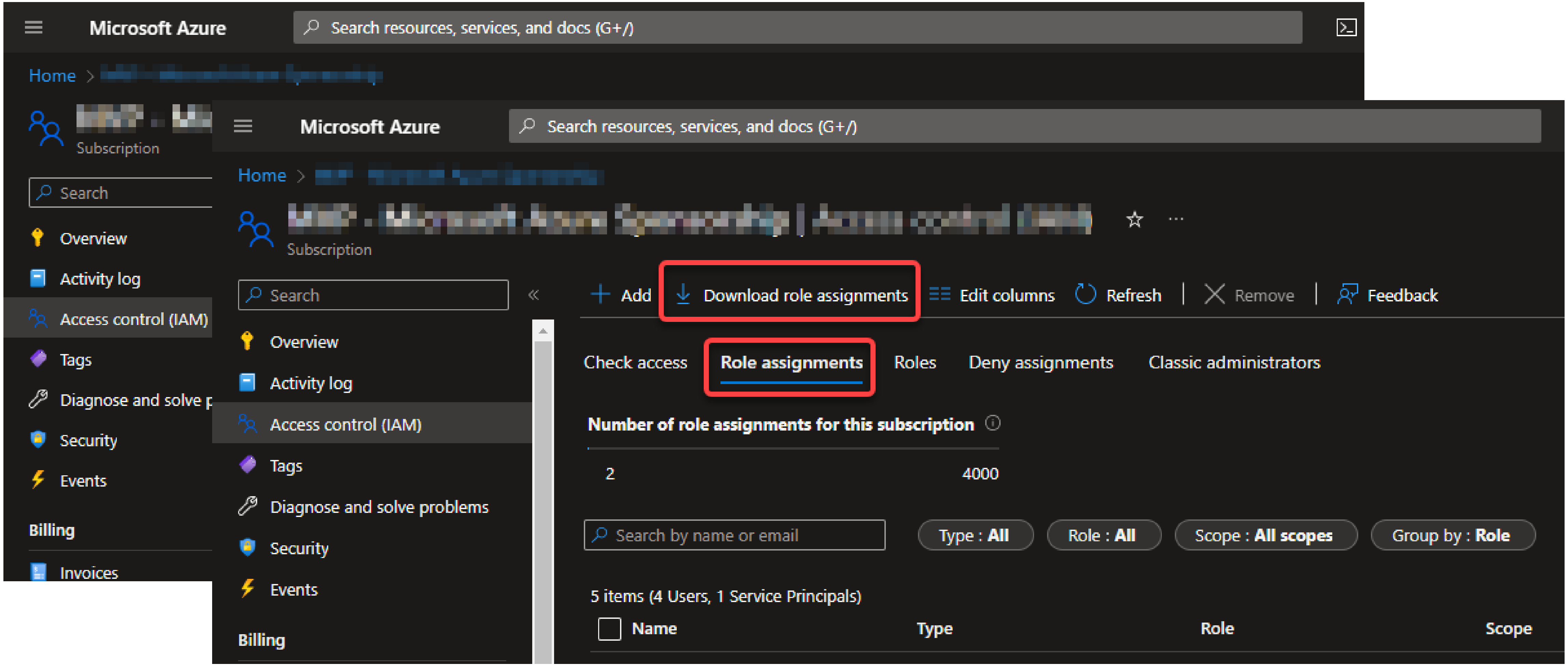
120 Developers
120 x 24 x 30 = 86.400 Hours

Active access after PIM:

15 activations daily (mon-fre)
15 x 8 x 22 = 2.640 Hours

Discovery?

What?



Number of role assignments for this subscription

2 4000

Search by name or email

Type : **All** Role : **All** Scope : **All scopes** Group by : **Role**

5 items (4 Users, 1 Service Principals)

□ Name	Type	Role	Scope

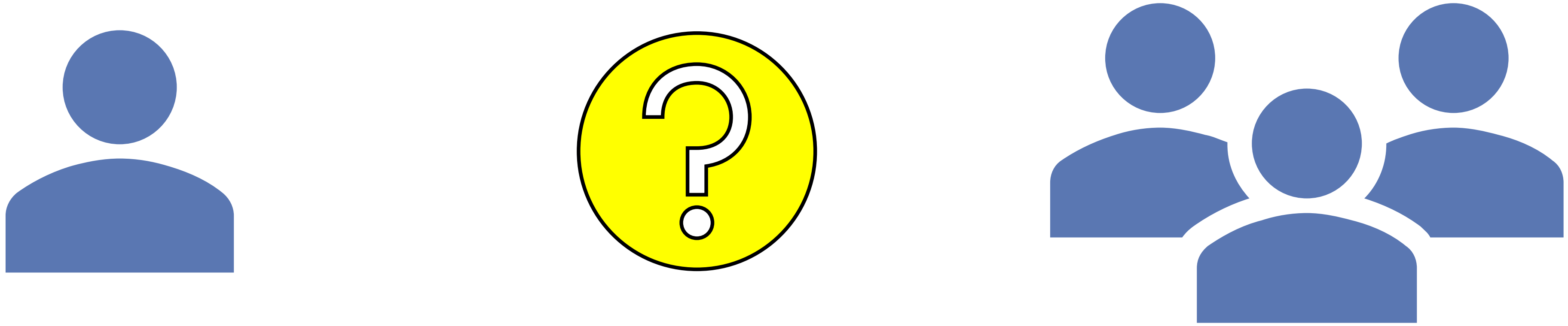
https://github.com/OTvedt/Scripts-For-Sharing/tree/master/Azure/PIM/Azure-resources/Document

- RolesUsedInSubs.ps1
- DocumentAllSubsAIM.ps1

Cleanup

SPAREBANKEN VEST

What?



https://github.com/OTvedt/Scripts-For-Sharing/tree/master/Azure/Access_Control_(IAM)

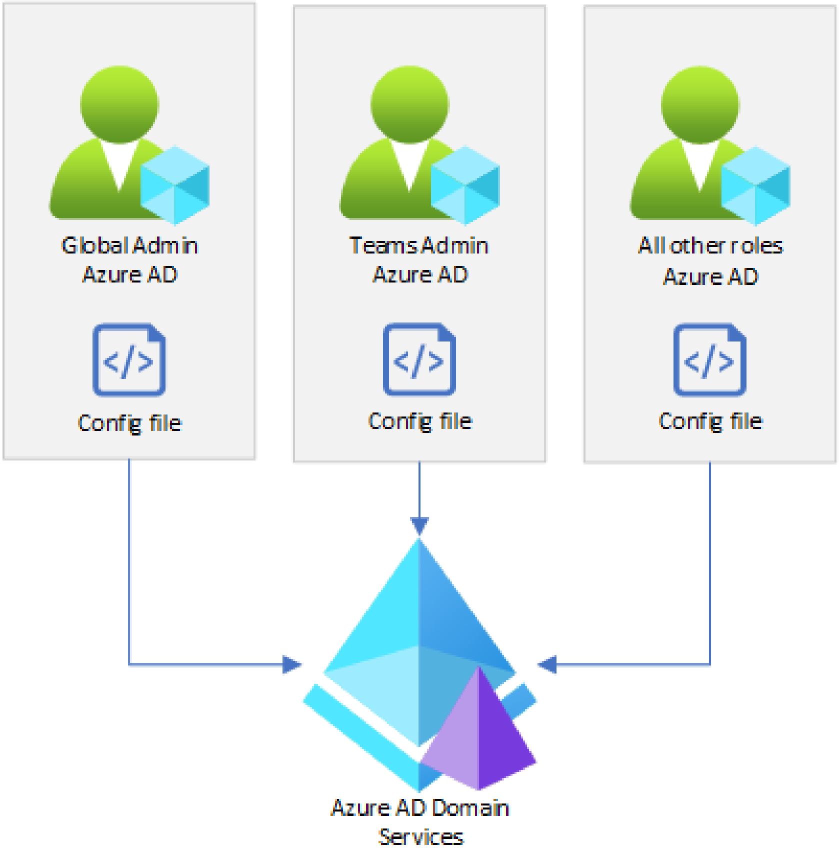
- Excel sheet
- Iam-removeunknown.ps1

Modify

SPAREBANKEN VEST

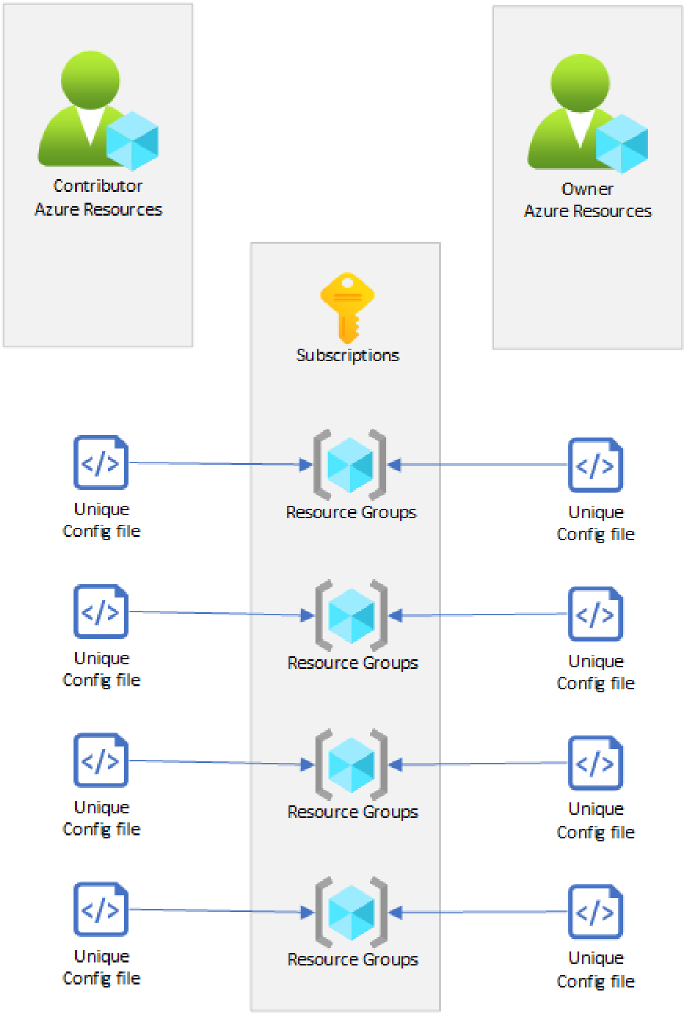
Why?

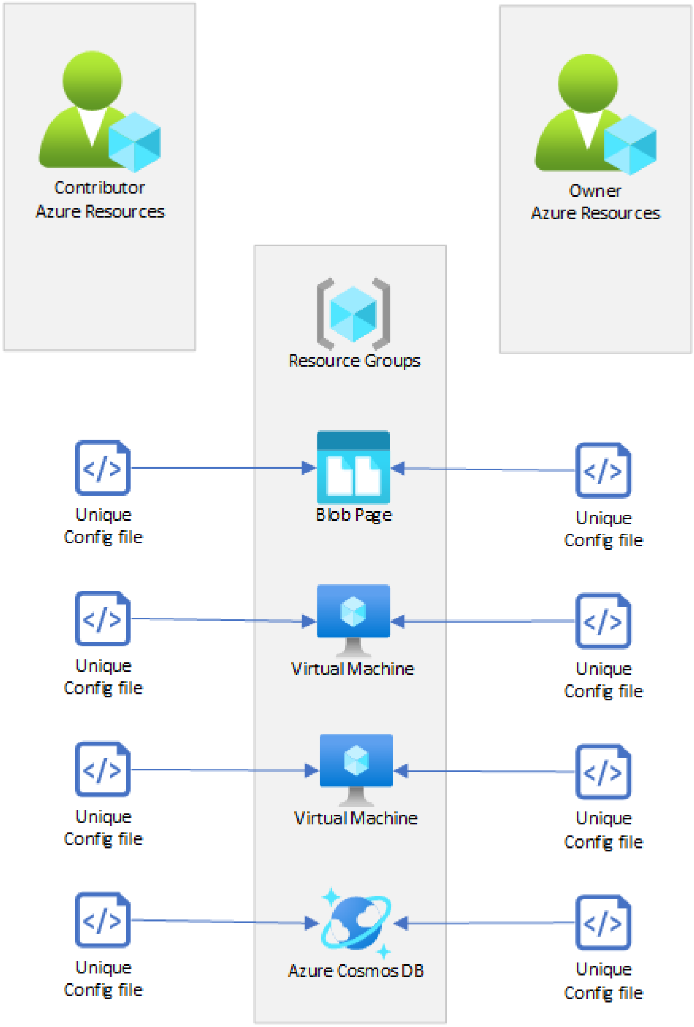
Azure AD role config



Why?

Azure Resources Config





https://github.com/OTvedt/Scripts-For-Sharing/tree/master/Azure/PIM/Azure-resources/Modify

- Pim-EditRoleInAllRGs.ps1
- Default-settings.json

Apply

https://github.com/OTvedt/Scripts-For-Sharing/tree/master/Azure/PIM/Azure-resources/Apply

- Pim-SetContributorEligibility.ps1
- Pim-AddReader.ps1

Common misunderstandings and problems

Common misunderstandings and problems

- Misunderstandings
  - It’s just the same as Azure AD PIM
  - It’s a replacement for groups

- Problems
  - Activation, token and refresh
  - Multiple browsers/Windows
  - My colleague has access, I want it too!
  - Scope
  - The realm between Contributor and Reader

- User Training
  - Portal
  - Script?

Olav Tvedt

SparebankenVest

- 15 x MVP
  - Setup & Deployment
  - Software Packaging, Deployment & Servicing
  - Windows Expert – IT Pro
  - Office and Applications
  - Cloud & Server Installation and Servicing
  - Cloud and Datacenter

olavtwitt

https://www.linkedin.com/in/otvedt/

https://olavtvedt.blogspot.com/

https://github.com/OTvedt/Scripts-For-Sharing

https://www.youtube.com/@bluescreenbrothers

Søk ellers etter BlåSkjerm Brødrene i din favoritt Podkast app eller Spotify