PERMISSIONS MANAGEMENT

What is the best way to do it in corporate?

Ilya Rokhkin | HC DevOps

Challenge

How many tickets a new employee

needs to open to get all access required?

Who Am I?

```yaml
---
name: Ilya
last_name: Rokhkin
married: true
kids: 3
title: DevOps Engineer
experience: 20 years
---
team: Harmony Connect DevOps
responsibility:
    - HC production, SRE, monitoring
    - HC DevEnv, CI/CD, cost, and much more …
    - Help to other DevOps teams
```
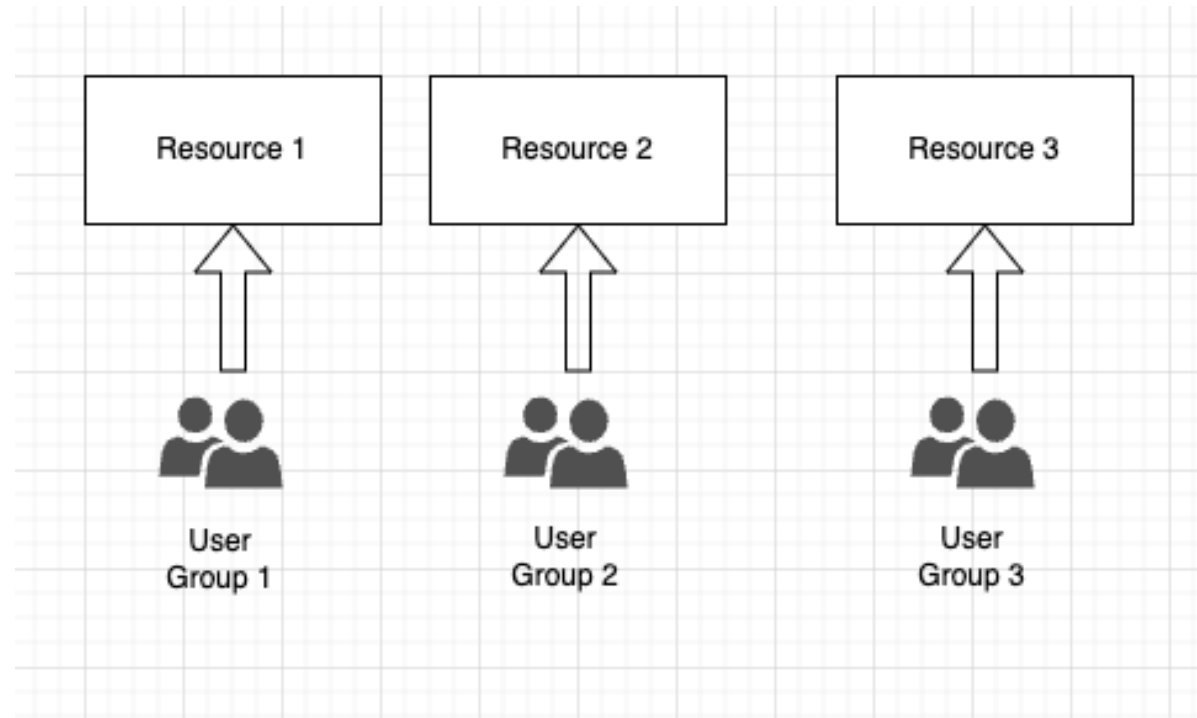
The story

- Up to 20 tickets to get access to AWS only

- Org AD groups were broken after reorgs and access was lost.

- People who moved to other groups still had access to production

- Access to production was given immediately
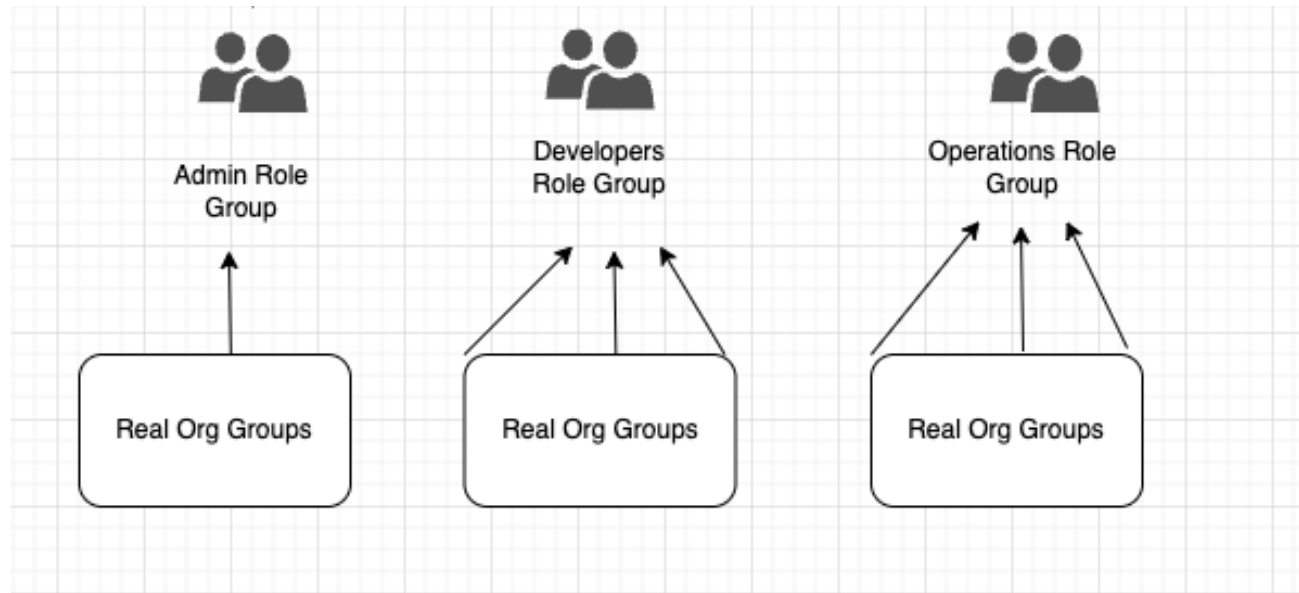
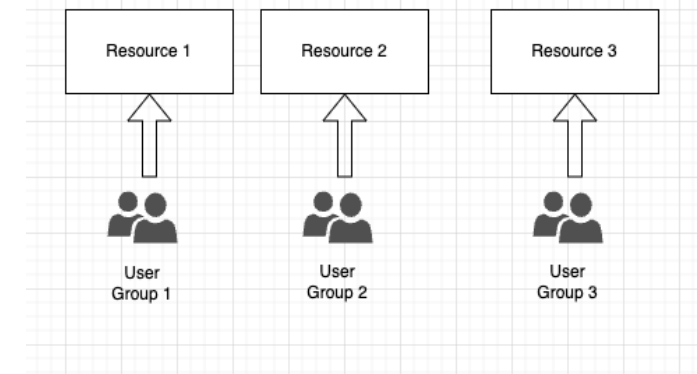- Org AD groups are often nested and can't give access

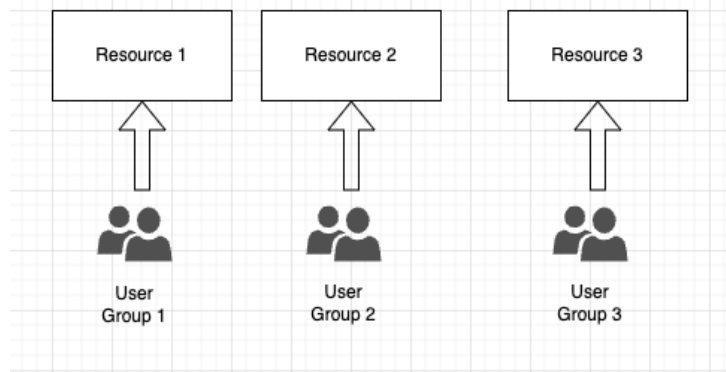# How it works – the group is giving access to the resource
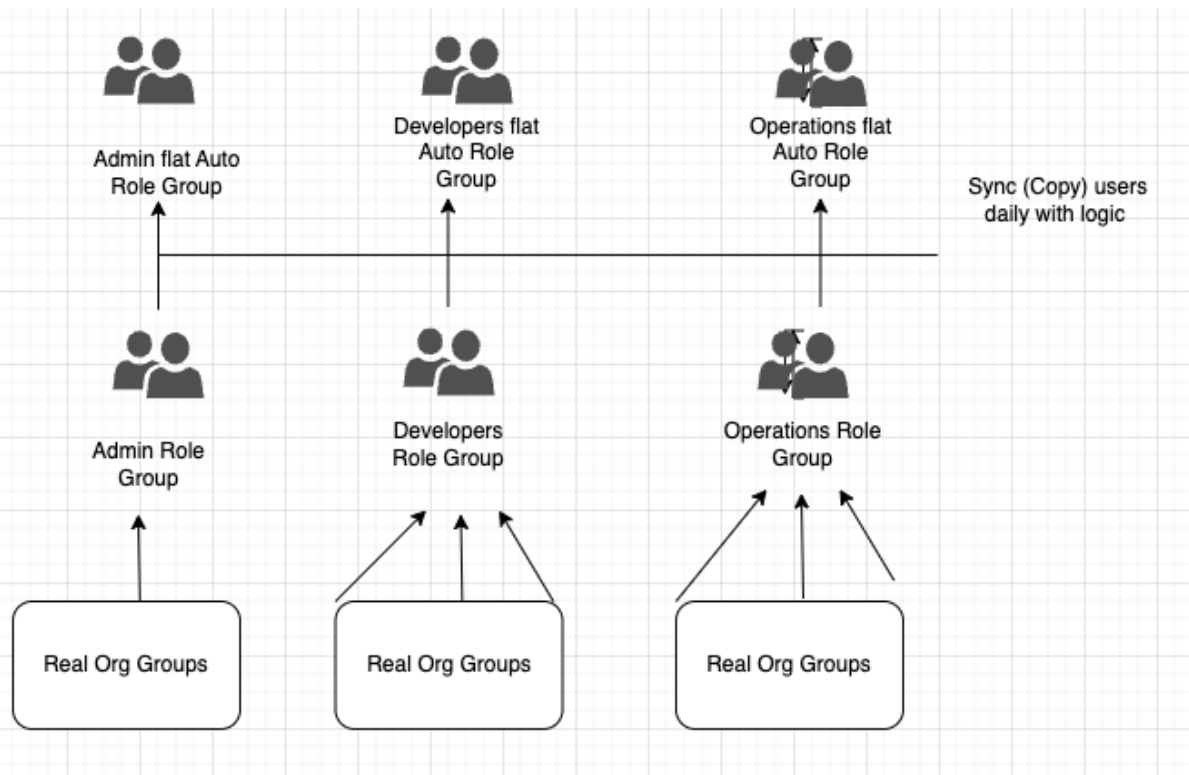
Current situation

Solution

Role Based groups templates
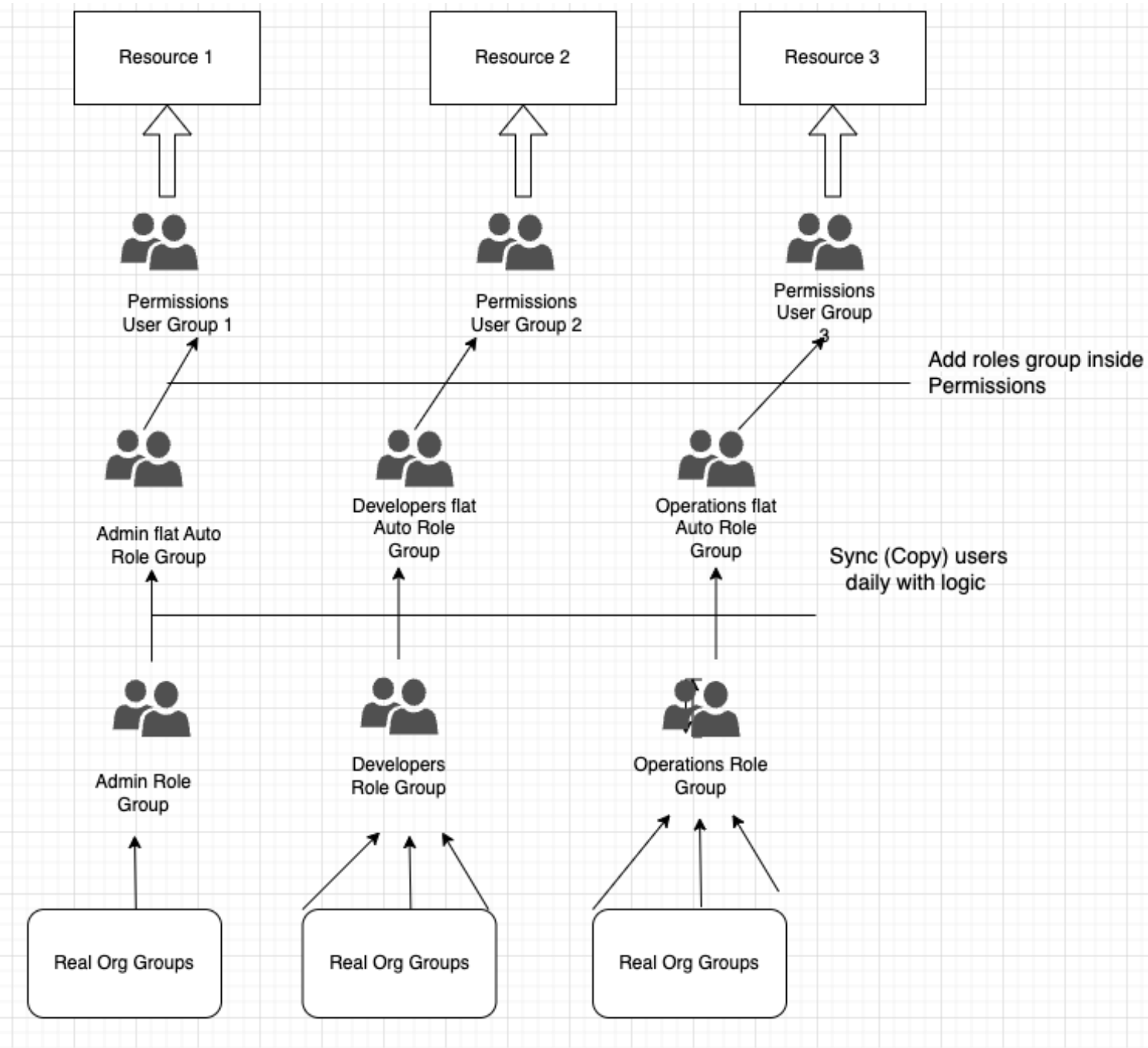
Solution

Role flat groups automatically synced - Smart Sync groups logic

- The sync adds new users and removes left users, (including internal moves)

- If more than 3 users intended to be removed, Smart Sync stops and notifies possible reorg

- Delay of addition to Admin and Operations group only after 10 days

The complete Solution

Resource 1

Resource 2

Resource 3

Permissions User Group 1

Permissions User Group 2

Permissions User Group 3

Admin flat Auto Role Group

Developers flat Auto Role Group

Operations flat Auto Role Group

Add roles group inside Permissions

Sync (Copy) users daily with logic

Admin Role Group

Developers Role Group

Operations Role Group

Real Org Groups

Real Org Groups

Real Org Groups

Summary

- New user gets all-needed access automatically to all resources without opening a single ticket to HD

- Access is stable and not influenced by reorgs

- Once we added our smart groups to resource groups, we do not depend on other groups MIS, HD, CloudInfra, etc. anymore

- PRD is safer as new users get access after some time automatically

- User that moves to another BU, her/his access is removed automatically

More Info

- For more info, please contact me: astra07_2010 at yahoo.com

Q & A

THANK YOU