2nd Annual

MidPoint Community Meetup

Workshop: Bring Your Own Problem

Evolveum

Radovan Semančík, Slávek Licehammer

May 2026

Workshop Overview

- This is a workshop, not tutorial
- Discussion is not just welcome, it’s necessary
- Your input can help with further midPoint development
- Five problems shared beforehand
  - We can explore broader context
- Bring ad-hoc problems
  - Only if time allows

Parallel development/configuration in midPoint

Deployment of changes in configuration from different people require a big coordination effort and sometimes changes are overwritten etc.

Parallel development/configuration in midPoint

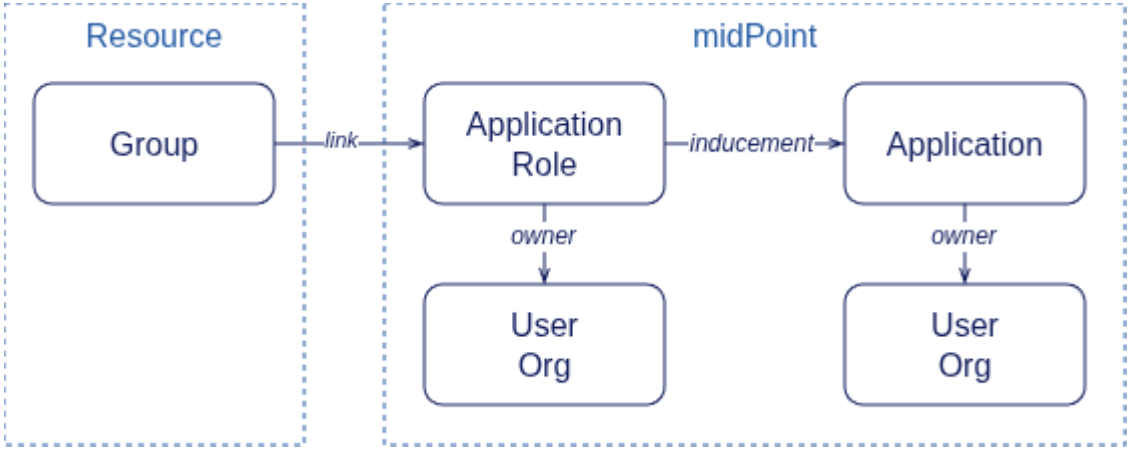
- Own testing environment for designing new configuration
- Synchronize only deployment to production
  - Consider service management processes
  - Technical limitation to only a single concurrent simulation
- midPoint studio diff capabilities
  - Prevents unwanted changes
- GitOps processes

Role design and maintenance

How do you ensure, that users know what roles/groups really do and keep that information up to date? Do you track the ownership of roles/groups by other business departments?

Entitlement Governance

- Sync entitlements to midPoint
  - groups → application roles
- Manage owners in midPoint
  - Note: owner can be an *org* instead of *user*
- “Require owner” policy rule
- “Require description” policy rule (demo)
- Certification of role definitions (inducements)
- Set legacy roles to *deprecated* lifecycle state
- Dashboard



Require Description

```
<policyRule>
  <policyConstraints>
    <objectState>
      <expression>
        <script>
          <language>...#mel</language>
          <code>
            isNull(object.?description)
            || isBlank(str(object.?description))
            || size(stringify(object.?description).trim()) &lt; 3
            || stringify(object.?description).matches('\\b(?i:TODO)\\b')
          </code>
        </script>
      </expression>
    </objectState>
  </policyConstraints>
  ...
```

Connecting to asynchronous systems

How to integrate asynchronous systems where provisioning is done using messaging or where API operations are not immediately executed?

Asynchronous source systems

- Asynchronous connector
  - Experimental
  - Reconciliation?
- Use async. messages to trigger import
- Caching resource objects
  - For resources which are not available all the time
  - Fully supported for import from 4.11

Asynchronous target systems

- Caching resource objects
  - Deals with delayed execution of changes
- Provisioning propagation
  - Schedule write operation
- Import changes using other channels (REST, hooks, ...)
  - Not recommended when not synchronised with resource data

Delegation to business owners and power-users

I'm trying to setup two layers of administration, so that regular admins can do everything at business level, while everything that is technical, and dangerous for the platform (including XML editing that has no power restriction) is only accessible to a super admin.

Delegated Administration

- Authorizations are very *flexible* and very *complex*
- Troubleshooting authorizations
  https://docs.evolveum.com/midpoint/reference/support-4.10/diag/troubleshooting/authorizations/
- Safe expressions with MEL (midPoint 4.11)
  https://docs.evolveum.com/midpoint/reference/master/expressions/expressions/script/mel/introduction/
- Goal: more pre-configured system roles in future midPoint releases
- Limitations
  - Limited GUI support
  - Authorization vs adminGuiConfig
  - XML editing: raw → only for superuser

LDAP: handling different object types simultaneously

How to handle LDAP with complex object schema, like using groupOfNames and posixGroups at the same time?

LDAP with complex schema

- Object types in schema handling
  - Objects need to be homogenous
- Multiple association definition
- Might require to fine tune association construction rules
- Watch for LDAP quirks


Evolveum
Thank you for your attention
Feel free to ask your questions now!
2nd Annual MidPoint Community Meetup