

# Evolveum



## Simulations

Pavol Mederly / December 2023  
Senior Software Developer

# Agenda

- Overview
- Demonstration
- Customization
- Tips and tricks
- Future developments



## An Overview

- Identity management is a complex field
- Full understanding of the data is scarce
- Results of actions can be hard to predict
- Configuration errors can be disastrous
- Testing environment is expensive, and sometimes unfeasible
- **Simulations**
  - Seeing the expected effects of actions in a safe way

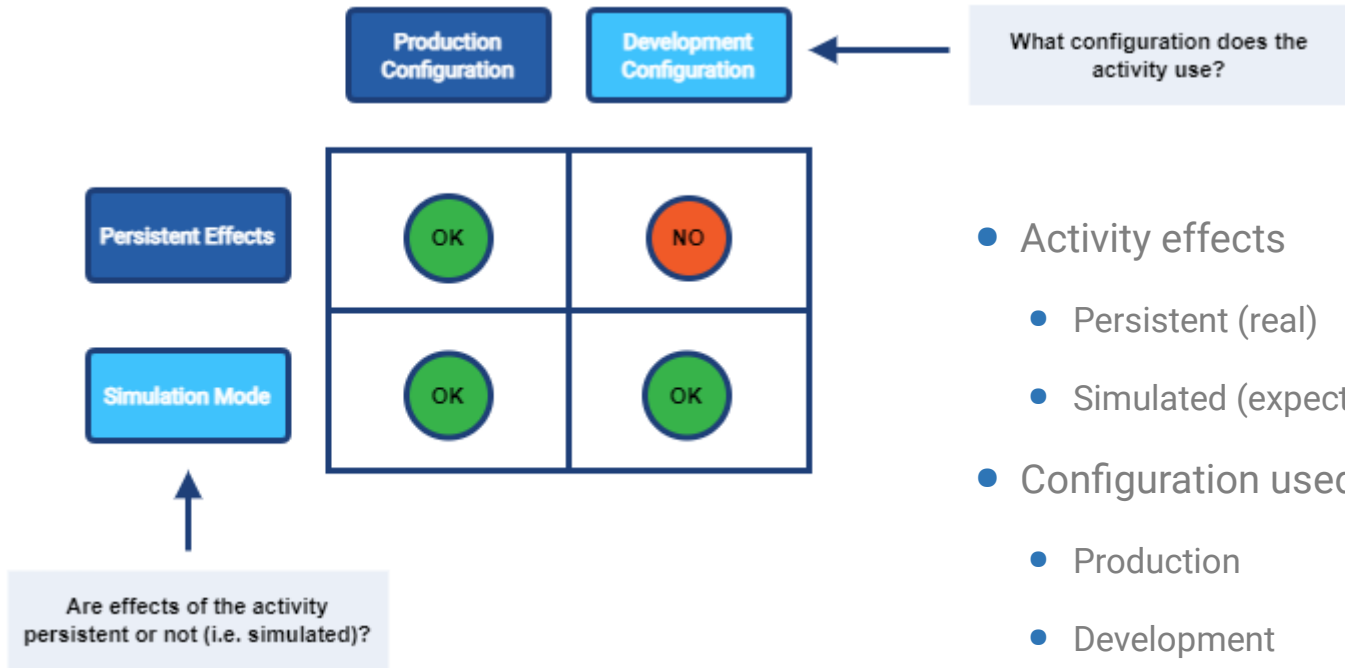


# Benefits of Simulations

- Faster connect/clean-up/automate cycle
  - **connect:** new systems are connected to midPoint more easily
  - **clean-up:** data quality can be improved more efficiently
  - **automate:** processes (including *joiners* and *leavers*) are implemented in shorter time
- Reducing the risk throughout the cycle
- No need for separate testing environment
- Also in operational stage
  - supporting reorganizations – *movers*
  - protect against unexpected events



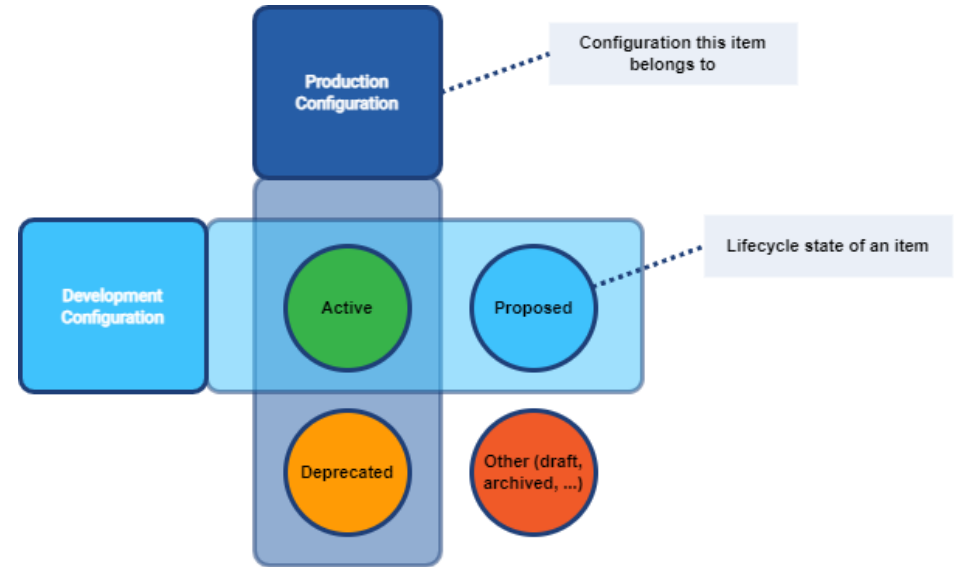
## Basic Terms



- Activity effects
  - Persistent (real)
  - Simulated (expected)
- Configuration used
  - Production
  - Development

# Production and Development Configuration

- Using the **lifecycle state** as a discriminator
  - production = active + deprecated
  - development = active + proposed
- Supported configuration items:
  - resource
  - resource object class and type
  - resource object attribute & association
  - synchronization reaction
  - abstract roles (role, org, service, archetype)
  - assignment and inducement
  - object template
  - mapping



**Short demo**

[← Back](#)

## Simulation result: Reconciliation task: OpenLDAP: Account/default (simulated), 2023-12-06T23:30:18.597+01:00

[View processed objects](#)

### ? Simulation task details

Start timestamp  
6 December 2023 at  
23:30:18 CET

End timestamp  
6 December 2023 at  
23:30:28 CET

Finished in  
10 seconds

Task  
Reconciliation task:  
OpenLDAP:  
Account/default  
(simulated)

Status  
**Finished**

Configuration  
Development

Added objects  
0

Deleted objects  
4

Modified objects  
490

Unmodified objects  
257

All processed objects  
751

Errors  
0

### ▼ Event marks

Focus activated

0

[More info →](#)

Focus deactivated

0

[More info →](#)

Focus renamed

0

[More info →](#)

Focus assignments changed

0

[More info →](#)

Focus archetype changed

0

[More info →](#)

Focus parent organization refer...

0

[More info →](#)

Focus role membership changed

0

[More info →](#)

Projection activated

0

[More info →](#)

Projection deactivated

4

[More info →](#)

Projection renamed

0

[More info →](#)

Projection identifier changed

0

[More info →](#)

Projection entitlement changed

39

[More info →](#)

Projection password changed

0

[More info →](#)

Resource object affected

249

[More info →](#)

LDAP account modified

249

[More info →](#)

LDAP service account modified

3

[More info →](#)

### ▼ Metrics

Attributes modified

546

Attributes modified per account

2.229

Ratio of LDAP accounts modified

0.984



# Reports

- Standard reports
  - All simulation results
  - Objects in the given simulation result (with/without metrics)
  - Items changed
  - Values changed



## Selected Parts of “Simulation Results” Report

Event mark	Explicit metric	Aggregation function	Scope: resource	Value	Selection size	Selection total value	Domain size	Domain total value
LDAP account modified		Selection total value	HR	0	0	0	249	0
LDAP account modified		Selection total value	OpenLDAP	249	249	249	253	249
LDAP service account modified		Selection total value	HR	0	0	0	249	0
LDAP service account modified		Selection total value	OpenLDAP	3	3	3	253	3
Projection activated		Selection total value	HR	0	0	0	249	0
Projection activated		Selection total value	OpenLDAP	0	0	0	253	0
Projection deactivated		Selection total value	HR	0	0	0	249	0
Projection deactivated		Selection total value	OpenLDAP	4	4	4	253	4
Projection entitlement changed		Selection total value	HR	0	0	0	249	0
Projection entitlement changed		Selection total value	OpenLDAP	39	39	39	253	39
Projection identifier changed		Selection total value	HR	0	0	0	249	0
Projection identifier changed		Selection total value	OpenLDAP	0	0	0	253	0
Projection password changed		Selection total value	HR	0	0	0	249	0
Projection password changed		Selection total value	OpenLDAP	0	0	0	253	0
Projection renamed		Selection total value	HR	0	0	0	249	0
Projection renamed		Selection total value	OpenLDAP	0	0	0	253	0
Resource object affected		Selection total value	HR	0	0	0	249	0
Resource object affected		Selection total value	OpenLDAP	249	249	249	253	249
	attribute-modifications	Selection total value	HR	0	0	0	249	0
	attribute-modifications	Selection total value	OpenLDAP	546	245	546	253	546
	ldap-accounts-modified-ratio	Selection size to domain size	OpenLDAP	0.984	249	249	253	249
	modifications-per-account-modified	Selection total value to selection size	HR		0	0	249	0
	modifications-per-account-modified	Selection total value to selection size	OpenLDAP	2.229	245	546	253	546

Name	Resource	State	Event mark	Explicit metric	Selecte	Valu
uid=dmarsden,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=ncathcar,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=telie,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=tcornish,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	3
uid=wlomax,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	3
uid=pstiller,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=cressler,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	3
uid=mblythe,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=lforney,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=msheley,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=mreeves,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=rshanaha,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=afrances,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=mattaway,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=byandegr,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=dtannehi,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=jquach,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=acusick,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=mstimpso,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=tjenning,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=jnecaise,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	3
uid=hlavoie,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	3
uid=tkifer,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=mescobed,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=oho,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=jgerald,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=vlam,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=rwunsch,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=cmoak,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=amcnicho,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2
uid=csilveir,ou=people,dc=example,dc=com	OpenLDAP	Modified		attribute-modifications	true	2

Name	Item changed	Old value(s)	New value(s)
<a href="#">uid=dmarsden,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Training	
<a href="#">uid=ncathcar,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Strategy - Planning	
<a href="#">uid=telie,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Professional Services	
<a href="#">uid=tcornish,ou=people,dc=example,dc=com</a>	<a href="#">attributes/mail</a>	<a href="#">cornish6@ext.example.org</a>	<a href="#">tcornish@example.org</a>
<a href="#">uid=tcornish,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Sales	
<a href="#">uid=wlomax,ou=people,dc=example,dc=com</a>	<a href="#">attributes/mail</a>	<a href="#">lomax4@ext.example.org</a>	<a href="#">wlomax@example.org</a>
<a href="#">uid=wlomax,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Inventory	
<a href="#">uid=pstiller,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Training	
<a href="#">uid=cressler,ou=people,dc=example,dc=com</a>	<a href="#">attributes/mail</a>	<a href="#">ressler6@ext.example.org</a>	<a href="#">cressler@example.org</a>
<a href="#">uid=cressler,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Business Development	
<a href="#">uid=mblythe,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Design	
<a href="#">uid=lforney,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Logistics	
<a href="#">uid=mshaley,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Marketing	
<a href="#">uid=mreeves,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Human Resources	
<a href="#">uid=rshanaha,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Professional Services	
<a href="#">uid=afrances,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Customer Service	
<a href="#">uid=mattaway,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Strategy - Planning	
<a href="#">uid=bvandegr,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Purchasing	
<a href="#">uid=dtannehi,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Accounting	
<a href="#">uid=jquach,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Quality Assurance	
<a href="#">uid=acusick,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Information Technology	
<a href="#">uid=mstimpso,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Inventory	
<a href="#">uid=tjenning,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Administration	
<a href="#">uid=jnecaise,ou=people,dc=example,dc=com</a>	<a href="#">attributes/mail</a>	<a href="#">necaise9@ext.example.org</a>	<a href="#">jnecaise@example.org</a>
<a href="#">uid=jnecaise,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Accounting	
<a href="#">uid=hlavoie,ou=people,dc=example,dc=com</a>	<a href="#">attributes/mail</a>	<a href="#">lavoie6@ext.example.org</a>	<a href="#">hlavoie@example.org</a>
<a href="#">uid=hlavoie,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Business Development	
<a href="#">uid=tkifer,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Training	
<a href="#">uid=mescobed,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Logistics	
<a href="#">uid=ofo,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Marketing	
<a href="#">uid=jgerald,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Warehouse	
<a href="#">uid=vlam,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Support Services	
<a href="#">uid=rwunsch,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Supply Chain	
<a href="#">uid=cmoak,ou=people,dc=example,dc=com</a>	<a href="#">attributes/ou</a>	Manufacturing	

# Simulation Metrics

## ▼ Event marks

Focus activated

0

[More info](#)

Focus deactivated

0

[More info](#)

Focus renamed

0

[More info](#)

Focus assignments changed

0

[More info](#)

Focus archetype changed

0

[More info](#)

Focus parent organization reference changed

0

[More info](#)

Focus role membership changed

0

[More info](#)

Projection activated

0

[More info](#)

Projection deactivated

4

[More info](#)

Projection renamed

0

[More info](#)

Projection identifier changed

0

[More info](#)

Projection entitlement changed

39

[More info](#)

Projection password changed

0

[More info](#)

Resource object affected

249

[More info](#)

LDAP account modified

249

[More info](#)

LDAP service account modified

3

[More info](#)

## ▼ Metrics

Attributes modified

546

Attributes modified per account

2.229

Ratio of LDAP accounts modified

0.984

## Customization: Metrics

Numeric values attached to individual processed objects or their aggregations

Type	Example	Values	Searchable	Customizable
built-in	added, deleted, modified	0 or 1	yes	no
event mark based	focus activated, deactivated	0 or 1	yes	yes
explicit (custom)	number of modifications	any number	not yet	yes

## Event Marks

- **Operations** can be **classified** by attaching **marks**
- Used by simulations, later: audit, dashboards
  - Meant to (eventually) replace policy situations
- Default set of marks provided
- Not to be confused with **object marks**

▼ Event marks		
Focus activated 0 <a href="#">More info</a>	Focus deactivated 0 <a href="#">More info</a>	Focus renamed 0 <a href="#">More info</a>
Focus assignments changed 0 <a href="#">More info</a>	Focus archetype changed 0 <a href="#">More info</a>	Focus parent organization ... 0 <a href="#">More info</a>
Focus role membership ch... 0 <a href="#">More info</a>	Projection activated 0 <a href="#">More info</a>	Projection deactivated 0 <a href="#">More info</a>
Projection renamed 0 <a href="#">More info</a>	Projection identifier changed 0 <a href="#">More info</a>	Projection entitlement cha... 0 <a href="#">More info</a>
Projection password chang... 0 <a href="#">More info</a>	Resource object affected 5 <a href="#">More info</a>	

## Example: “Focus Renamed” Mark

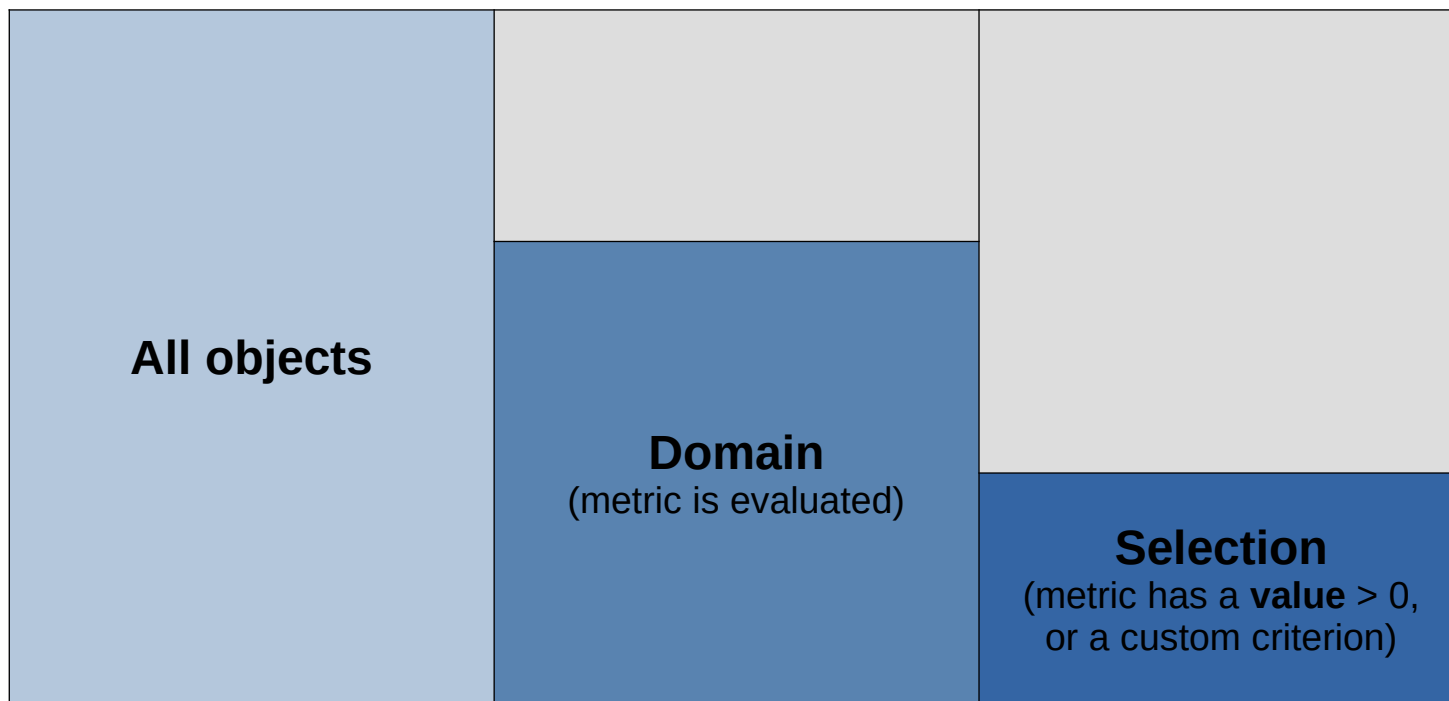
```
<mark xmlns="http://midpoint.evolveum.com/xml/ns/public/common/common-3"
      oid="00000000-0000-0000-0000-000000000712">
  <name>Focus renamed</name>
  <description>Operation that renamed the focus</description>
  <assignment>
    <targetRef oid="00000000-0000-0000-0000-000000000700" type="ArchetypeType"/>
  </assignment>
  <displayOrder>120</displayOrder>
  <policyRule>
    <policyConstraints>
      <modification>
        <operation>modify</operation>
        <item>name</item>
      </modification>
    </policyConstraints>
  </policyRule>
</mark>
```



## Example: "Service Account Modified" Mark

```
<mark xmlns="http://midpoint.evolveum.com/xml/ns/public/common/common-3"
      xmlns:ri="http://midpoint.evolveum.com/xml/ns/public/resource/instance-3"
      xmlns:q="http://prism.evolveum.com/xml/ns/public/query-3"
      oid="5dbdc23e-2135-4537-ac97-d47bc066fa46">
  <name>Service account modified</name>
  <assignment>
    <targetRef oid="00000000-0000-0000-0000-000000000700" type="ArchetypeType"/> ←!— event mark →
  </assignment>
  <displayOrder>900</displayOrder> ←!— show this mark at the end →
  <policyRule>
    <policyConstraints>
      <objectState>
        <filter>
          <q:text>resourceRef matches (oid = '32531590-4606-4333-9cc2-0faa1ae68509')</q:text> ←!— LDAP →
        </filter>
      </objectState>
      <objectState>
        <filter>
          <q:text>attributes/ri:employeeType = "service"</q:text>
        </filter>
      </objectState>
      <or> ←!— copied from "resource object affected" event mark →
        <modification>
          <operation>modify</operation>
          <specialItem>resourceObjectItem</specialItem>
        </modification>
        <modification>
          ←!— We assume that ADD/DELETE always modifies the state of the resource →
          <operation>add</operation>
          <operation>delete</operation>
        </modification>
      </or>
    </policyConstraints>
    <evaluationTarget>projection</evaluationTarget>
  </policyRule>
</mark>
```

## Metric Domain, Selection, and Value



## Custom Metric Definition

```
<metric>
  <identifier>attribute-modifications</identifier>
  <display>
    <label>Attributes modified</label>
  </display>
  <computation>
    <domain>
      <expression>
        <script>
          <code>processedObject.shadow</code>
        </script>
      </expression>
    </domain>
    <valueExpression>
      <script>
        <code>processedObject.attributeModificationsCount</code>
      </script>
    </valueExpression>
  </computation>
</metric>
```

# Metrics Aggregation

```
<metric>
  <identifier>modifications-per-account-modified</identifier>
  <display>
    <label>Attributes modified per account</label>
  </display>
  <aggregation>
    <aggregationFunction>selectionTotalValueToSelectionSize</aggregationFunction>
    <source>
      <identifier>attribute-modifications</identifier>
    </source>
  </aggregation>
</metric>
```

## ▼ Metrics

Attributes modified

**546**

Attributes modified per account

**2.229**

## Metrics Aggregation

Aggregation function	Description
selectionSize	number of objects selected by this metric
selectionTotalValue	sum of metric values for all objects selected by this metric
domainSize	number of objects in the domain of this metric
domainTotalValue	sum of metric values for all objects in the domain of this metric
domainTotalValueToDomainSize	$\text{domainTotalValue} / \text{domainSize}$
selectionTotalValueToDomainSize	$\text{selectionTotalValue} / \text{domainSize}$
selectionTotalValueToSelectionSize	$\text{selectionTotalValue} / \text{selectionSize}$
selectionSizeToDomainSize	$\text{selectionSize} / \text{domainSize}$
selectionTotalValueToDomainTotalValue	$\text{selectionTotalValue} / \text{domainTotalValue}$
domainMinValue	minimal metric value in the domain
selectionMinValue	minimal metric value in the selection
domainMaxValue	maximum metric value in the domain
selectionMaxValue	maximum metric value in the selection

# How to Run Simulations

- On **foreground**
  - GUI: “**import preview**” (development or production)
  - GUI: “**preview changes**” (production only)
  - API: `ModelInteractionService.executeWithSimulationResult`
- On **background**
  - Synchronization, recomputation, scripting, change execution activities
  - GUI: various places where tasks are created
  - Via task settings:
    - `activity/execution/mode` (full, preview)
    - `activity/execution/configurationToUse` (production, development)
    - `activity/reporting/simulationResult` (enabled, definition)



## Tips and Tricks: Replacing Configuration Items

- Simulating configuration items replacement
  - Create a clone of the item in the “proposed” state
  - Original item set to “deprecated”
- It can be used for the majority of mappings, all assignments, inducements, synchronization reactions, and object templates (using a workaround)
- For others, the recommended way is to replace just the relevant parts



## Tips and Tricks: Avoiding Unsafe Operations

- Beware of a custom code!
- Stay with documented API, do not call lower-level APIs
  - `midpoint.*` methods are OK (except for two of them, see docs)
- Avoid actions outside `midPoint`: files, sockets, ...
- Use `task.getExecutionMode()` to check if necessary





## Limitations

- Simulated changes are just recorded, not used for subsequent operations
  - Create-on-demand is reported multiple times
- Multi-node tasks are not supported
- Approvals and notifications are skipped



## Future Work: Shadow Management Simulation

- Allows simulating shadow classification and correlation processes
- Synchronization is always skipped in this mode
- Experimental because of minor usability limitations



## Future Work: Others

- Overcoming the limitations
- Better support for role management
- Policy-based validation of input data
- Reducing the amount of data



## Conclusion

- Simulations feature is a powerful tool to be used when developing, maintaining, and operating a midPoint-based solution
- Speed, confidence, safety
- Powerful configuration options
- For more information, please see
  - <https://docs.evolveum.com/midpoint/reference/simulation/>
  - First Steps Methodology webinar by Ivan Noris:  
[https://www.youtube.com/watch?v=suo775ym\\_PE](https://www.youtube.com/watch?v=suo775ym_PE)



## Next Webinars

- Upgrade with Ninja, January 25, 2024
- **More webinars coming in 2024**



## Meet us at TIIME

- Jan 29 - Feb 01, 2024, Copenhagen, Denmark
- MidPoint Working Group (Jan 29 – 30)
  - 3 workshops and lot of the presentations
- See the [agenda](#)
- Call for speakers
  - Contact us at [marketing@evolveum.com](mailto:marketing@evolveum.com)
- Register here: <https://tiime-unconference.eu/>



# Thank you for your attention

Do you have any **questions**? Feel free to contact us at [info@evolveum.com](mailto:info@evolveum.com)

**Follow us** on social media or **join us** at GitHub or Gitter!



/Evolveum



@Evolveum



/Evolveum



/Evolveum



/Evolveum



/Evolveum

**Evolveum**

© 2023 Evolveum s.r.o. All rights reserved.