Evolveum

Integration with ID Match API

Current progress of development

Slavek Licehammer, Pavol Mederly / February 2022

Starting point

- midPoint up to 4.4.

  - Correlate users with accounts on resources

  - Programmable correlation rules

  - Partial match not supported

  - Disputed status is hard to resolve

- ID Match API

  - API for identity matching

- COmanage Match

  - Implementation of ID Match API

  - Matching rules are defined there

Goals

Evolveum

- **Integrate ID Match API with midPoint**

- Use ID Match API for account correlation

- Use COmanage Match for testing the integration

- Enhance account correlation features

- Keep everything well integrated in midPoint

- Mind overall performance

Current status

- Development in progress

- First functional prototype

- Standard workflow fully supported

- Corner cases might not work yet

- GUI is the first prototype

  - Will be subject of changes in the future

Design choices

- Correlation of users instead of accounts

  - Human-friendly

  - All additional details available

- Account attributes are converted to midPoint schema

  - Easier correlation across resources

  - Human-friendly (e.g. DN vs. Username)

- Use single SoR "midPoint" in ID Match API

  - Resource identifier encoded in SoR ID attribute in ID Match API

- Solution is usable for all objects (not only users)

1) Import (reconciliation, …) of an account

2) Apply inbound mappings -> partial User object

3) ID Match API query

   1) Get back reference ID(s)

4) Account is „linked" or stays „disputed"

5) Resolving disputed state

   1) Resolve the case in midPoint (that will resolve it automatically in COmanage Match)

   2) Resolve pending match in COmanage Match and re-import (or reconcile) the account

- Two source systems: SIS, HR (CSV files)

  - Attributes: given name, family name, date of birth, national ID

  - Subtle differences in schema

- ID Match rules

  - **All attributes match -> automatic correlation (implicit)**

  - National ID, date of birth and family name matches -> automatic correlation

  - National ID matches -> manual correlation

  - Date of birth, given name and family name matches -> manual correlation

  - **No previous match -> new user (implicit)**

DEMO

(live demo is replaced by screenshots)

Correlation with single candidate account (owned by a single user)

SELF SERVICE

- Home
- Profile
- Credentials
- Request a role

ADMINISTRATION

- Dashboards
- Users
- Org. structure
- Roles
- Services
- Resources
- Cases **1**
- Certification
- Server tasks
- Nodes
- Reports

Configuration

- Archetypes
- Object collections
- Object templates

Correlation of account '4'

✔ Correlation case

Operations

← Back | 💾 Save | 🗑 Delete object | ✏ Edit raw

Case operations

■ Stop process

	Basic					

● Basic		**Object being correlated**	**Correlation candidate 1**
○ Correlation	**Action**	Create new	Correlate
○ Workitems **1**			
	Name		👤 John Smith (smith2)
	Given name	John	John (Ian)
	Family name	Smith	Smith
	Date of birth	2004-02-06	2004-02-06
	National ID	040206	040206/1328

Matchgrid: demo 🔧

COmanage™

- 🏠 Manage
- ☰ Display
- ✅ Reconcile
- ⚙ Configure

COmanage Match > demo > Pending Requests > Reconcile Unresolved Request midpoint/sis-4

Reconcile Unresolved Requests

	New Record	Suggestion 1
Reference ID	New	f9a13043-2d5d-4316-ad86-0196e6bbf24d
Action	GENERATE NEW REFERENCE ID	ASSIGN THIS REFERENCE ID
id	4	2
sor	midpoint	midpoint
sorid	sis-4	sis-2
request_time	2022-02-01 16:54:44	2022-02-01 16:54:22
resolution_time		2022-02-01 16:54:22
givenname	John	John
familyname	Smith	Smith
dateofbirth	2004-02-06	2004-02-06
nationalid	040206	040206/1328

SELF SERVICE ⌄

🎛 Home

👤 Profile

🛡 Credentials

📝 Request a role

ADMINISTRATION ⌄

🎛 Dashboards ‹

👤 Users ‹

📦 Org. structure ‹

👥 Roles ‹

☁ Services ‹

🗄 Resources ‹

〽 Cases [1]

✱ Certification ‹

▦ Server tasks ‹

▤ Nodes ‹

◔ Reports ‹

Configuration ⌄

⚲ Archetypes ‹

▼ Object collections ‹

▤ Object templates ‹

Correlation of account '5'

☑ Correlation case

Operations

← Back　💾 Save　🗑 Delete object　✎ Edit raw

Case operations

▪ Stop process

	Object being correlated	Correlation candidate 1
● Basic		
○ Correlation		
○ Workitems [1]		
Action	Create new	Correlate
Name		👤 Mary Smith (smith1)
Given name	Mary	Mary
Family name	Smith	Smith
Date of birth	2006-04-11	2006-04-10
National ID	060410/1993	060410/1993

Matchgrid: demo ⚙ COmanage™

- 🏠 Manage
- ☰ Display
- ● Reconcile
- ⚙ Configure

Reconcile Unresolved Requests

	New Record	Suggestion 1
Reference ID	New	cdae7a0d-f567-40f8-98d8-53910fcebe7b
Action	GENERATE NEW REFERENCE ID	ASSIGN THIS REFERENCE ID
id	5	1
sor	midpoint	midpoint
sorid	sis-5	sis-1
request_time	2022-02-01 17:03:08	2022-02-01 16:54:21
resolution_time		2022-02-01 16:54:21
givenname	Mary	Mary
familyname	Smith	Smith
dateofbirth	2006-04-11	2006-04-10
nationalid	060410/1993	060410/1993

Correlation with two candidate accounts owned by a single user

SELF SERVICE ∨

🎛 Home

👤 Profile

🛡 Credentials

✏ Request a role

ADMINISTRATION ∨

🎛 Dashboards ‹

👤 Users ‹

📦 Org. structure ‹

👥 Roles ‹

☁ Services ‹

🗄 Resources ‹

⇅ Cases 1

✱ Certification ‹

🖥 Server tasks ‹

🖳 Nodes ‹

◔ Reports ‹

Configuration ∨

⚲ Archetypes ‹

▼ Object collections ‹

📄 Object templates ‹

✔ Correlation of account '6'   ☑ Correlation case

Operations   **Case operations**

← Back   💾 Save   🗑 Delete object   ✏ Edit raw   ⬛ Stop process

● Basic		**Object being correlated**	**Correlation candidate 1**
○ Correlation	**Action**	Create new	Correlate
○ Workitems 1			
	Name		👤 John Smith (smith2)
	Given name	John	John (Ian)
	Family name	Smith	Smith
	Date of birth	2004-02-06	2004-02-06
	National ID	040206/8824	040206/1328 (040206)

Matchgrid: demo

COmanage ™

Manage

Display

Reconcile

Configure

Reconcile Unresolved Requests

	New Record	Suggestion 1	Suggestion 2
Reference ID	New	f9a13043-2d5d-4316-ad86-0196e6bbf24d	f9a13043-2d5d-4316-ad86-0196e6bbf24d
Action	GENERATE NEW REFERENCE ID	ASSIGN THIS REFERENCE ID	ASSIGN THIS REFERENCE ID
id	6	2	4
sor	midpoint	midpoint	midpoint
sorid	sis-6	sis-2	sis-4
request_time	2022-02-01 17:03:58	2022-02-01 16:54:22	2022-02-01 16:54:44
resolution_time		2022-02-01 16:54:22	2022-02-01 17:03:12
givenname	John	John	John
familyname	Smith	Smith	Smith
dateofbirth	2004-02-06	2004-02-06	2004-02-06
nationalid	040206/8824	040206/1328	040206

Correlation with three candidate accounts owned by two users

midPoint

SELF SERVICE ⌄

- 🖰 Home
- 👤 Profile
- 🛡 Credentials
- ☑ Request a role

ADMINISTRATION ⌄

- 🖰 Dashboards ‹
- 👤 Users ‹
- 🏢 Org. structure ‹
- 👥 Roles ‹
- ☁ Services ‹
- 🗄 Resources ‹
- ⟆ Cases 1
- ✹ Certification ‹
- ▦ Server tasks ‹
- ▤ Nodes ‹
- ◗ Reports ‹

Configuration ⌄

- ⚲ Archetypes ‹
- ▼ Object collections ‹
- ▤ Object templates ‹

Correlation of account 'A1003'

✔ Correlation case

Operations
← Back   💾 Save   🗑 Delete object   ☑ Edit raw

Case operations
▪ Stop process

	Object being correlated	Correlation candidate 1	Correlation candidate 2
● Basic			
○ Correlation			
○ Workitems 1			
Action	Create new	Correlate	Correlate
Name		👤 John Smith (smith3)	👤 John Smith (smith2)
Given name	John	John	John (Ian)
Family name	Smith	Smith	Smith
Date of birth	2004-02-06	2004-02-06	2004-02-06 (2004-02-26)
National ID	040206/2238	040206/8824	040206/1328 (040206)

Matchgrid: demo

COmanage™

🏠 Manage

☰ Display

✓ Reconcile

⚙ Configure

Reconcile Unresolved Requests

	New Record	Suggestion 1	Suggestion 2	Suggestion 3
Reference ID	New	f9a13043-2d5d-4316-ad86-0196e6bbf24d	f9a13043-2d5d-4316-ad86-0196e6bbf24d	7946e23a-972a-4454-bdfa-bbbf902d7c02
Action	GENERATE NEW REFERENCE ID	ASSIGN THIS REFERENCE ID	ASSIGN THIS REFERENCE ID	ASSIGN THIS REFERENCE ID
id	9	2	4	6
sor	midpoint	midpoint	midpoint	midpoint
sorid	hr-A1003	sis-2	sis-4	sis-6
request_time	2022-02-01 17:06:10	2022-02-01 16:54:22	2022-02-01 16:54:44	2022-02-01 17:03:58
resolution_time		2022-02-01 16:54:22	2022-02-01 17:03:12	2022-02-01 17:04:51
givenname	John	John	John	John
familyname	Smith	Smith	Smith	Smith
dateofbirth	2004-02-06	2004-02-06	2004-02-06	2004-02-06
nationalid	040206/2238	040206/1328	040206	040206/8824

Correlation with two candidate
accounts owned by a single user

Matched using non-primary
attribute value

midPoint

SELF SERVICE

- Home
- Profile
- Credentials
- Request a role

ADMINISTRATION

- Dashboards
- Users
- Org. structure
- Roles
- Services
- Resources
- Cases **1**
- Certification
- Server tasks
- Nodes
- Reports

Configuration

- Archetypes
- Object collections
- Object templates

Correlation of account 'A1001'

Correlation case

Operations

Back | Save | Delete object | Edit raw

Case operations

Stop process

	Basic	
	Correlation	
	Workitems	**1**

	Object being correlated	Correlation candidate 1
Action	Create new	Correlate
Name		John Smith (smith2)
Given name	Ian	John (Ian)
Family name	Smith	Smith
Date of birth	2004-02-26	2004-02-06
National ID	040206/1328	040206/1328 (040206)

END OF DEMO

Next steps

- Look and feel

- Reconciliation with COmanage Match database

- Productize the current prototype

- Documentation

Open questions

- Would anyone use ID Match API with accounts which are not in midPoint?

- Is it OK to correlate users instead of accounts?

- Does automatic unlinking need to be supported?

- Did this demo cover all your use-cases?

Thank you for attention

If any questions occur, feel free to ask at **slavek@evolveum.com**

Also **follow us** on our social media for further information!

/Evolveum   /Evolveum   /Evolveum   @Evolveum   /Evolveum

Evolveum