What's Hot In MidPoint

MidPoint User Group

TIIME Workshop

Vienna, January 2020

Agenda

- What’s hot
- Planning Yesterday
- Planning Today
- Planning Tomorrow

Evolveum

What’s Hot In MidPoint – Plan 4.1

- Flexible authentication
- UX improvements (Object collection/views, archetype, indirect assignments, …)
- Service management
- I2 grouper integration
- Split AD and Powershell connector
- Rewrite task pages – list and details
- Remove SOAP

Evolveum

What's Hot In MidPoint – Reality 4.1

- Flexible authentication
- UX improvements (Object collection/views, archetype, indirect assignments, …)
- Service management
- I2 grouper integration
- Split AD and Powershell connector
- Rewrite task pages – list and details
- ~~Remove SOAP~~

Evolveum

Flexible authentication

- Configurable as password policies in midPoint
- Different requirements for self-service and administration
- Advantage of account linking
- Using ConnId authenticate()
- Authentication module chaining

Evolveum

Flexible authentication

```
<modules>
    <loginForm id="1">
        <name>internalLoginForm</name>
        <description>Internal username/password authentication, default user password, login
        form</description>
    </loginForm>
    <httpBasic id="2">
        <name>internalBasic</name>
        <description>Internal username/password authentication, using HTTP basic
        auth</description>
    </httpBasic>
    <saml2 id="3">
        <name>mySamlSso</name>
        <description>My internal enterprise SAML-based SSO system.</description>
        <network>
            <readTimeout>10000</readTimeout>
            <connectTimeout>5000</connectTimeout>
        </network>
        <serviceProvider>
        ....
        </serviceProvider>
    </saml2>
```

Evolveum

Flexible authentication

```
<modules>
    <loginForm id
        <name>int
        <descript
        form</des
    </loginForm>
    <httpBasic id
        <name>int
        <descript
        auth</des
    </httpBasic>
    <saml2 id="3"
        <name>myS
        <descript
        <network>
            <read
            <conn
        </network
        <serviceP
        ....
        </service
    </saml2>
```

```
<mailNonce id="4">
    <name>registrationMail</name>
    <description>Authentication based on mail message with a nonce. Used for user
    registration.</description>
    <credentialName>mailNonce</credentialName>
</mailNonce>
<smsNonce id="5">
    <name>passwordResetSms</name>
    <description>Authentication based on SMS message with a nonce. Used for password
    resets.</description>
    <credentialName>smsNonce</credentialName>
    <c:mobileTelephoneNumberItemPath>extension/mobile</c:mobileTelephoneNumberItemPath>
</smsNonce>
<securityQuestionsForm id="6">
    <name>SecQ</name>
    <description>
        This is interactive, form-based authentication by using security questions.
    </description>
</securityQuestionsForm>
<httpSecQ id="7">
    <name>httpSecQ</name>
    <description>
        Special "HTTP SecQ" authentication based on security question answers.
        It is used for REST service.
    </description>
</httpSecQ>
```

Evolveum

Flexible authentication

```
<sequence id="8">
    <name>admin-gui-default</name>
    <description>
        Default GUI authentication sequence.
        We want to try company SSO, federation and internal. In that order.
        Just one of them needs to be successful to let user in.
    </description>
    <channel>
        <channelId>http://midpoint.evolveum.com/xml/ns/public/model/channels-
        3#user</channelId>
        <default>true</default>
    </channel>
    <module id="12">
        <name>mySamlSso</name>
        <order>30</order>
        <necessity>sufficient</necessity>
    </module>
    <module id="13">
        <name>internalLoginForm</name>
        <order>20</order>
        <necessity>sufficient</necessity>
    </module>
</sequence>
```

Evolveum

Flexible authentication

```
<sequence id="9">
    <name>admin-gui-emergency</name>
    <description>
        Special GUI authentication sequence that is using just the internal user password.
        It is used only in emergency. It allows to skip SAML authentication cycles, e.g. in
        case
        that the SAML authentication is redirecting the browser incorrectly.
    </description>
    <channel>
        <channelId>http://midpoint.evolveum.com/xml/ns/public/model/channels-
        3#user</channelId>
        <default>false</default>
        <urlSuffix>emergency</urlSuffix>
    </channel>
    <requireAssignmentTarget oid="00000000-0000-0000-0000-000000000004"
    relation="org:default" type="c:RoleType">
        <!-- Superuser -->
    </requireAssignmentTarget>
    <module id="14">
        <name>internalLoginForm</name>
        <order>30</order>
        <necessity>sufficient</necessity>
    </module>
</sequence>
```

Evolveum

Task Pages

Refreshing each 60 sec

Show subtasks | All execution states | All categories

Name	Category		Object reference	Execution	Executing at	Progress	Current run time	Scheduled to start again	Status
Cleanup	System			Runnable		2		in 3 hours 39 minutes 16 seconds	
Live Sync: LDAP Server (OpenLDAP)	Live synchronization		LDAP Server (OpenLDAP) over new LDAPConn.	Running	DefaultNode	876		runs continually	
Trigger Scanner	System			Runnable		0/0		in 4 minutes 16 seconds	
Validity Scanner	System			Runnable		0/0		in 9 minutes 16 seconds	

1 to 4 of 4 << < 1 > >>

Evolveum

Task Pages

Name: All | More... | Advanced

		Name	Category	Execution	Object reference	Executing at	Current run time	Scheduled to start again	Progress	Status	
☐		Cleanup	System	Runnable					0	✓	
☐		Execution of Approving and executing change of user "g.lockhart" (started Jul 28, 2019 12:21:26 PM)	Workflow	Suspended	ab5f2e8d-d0f2-4fda-a63f-003e36749cda				0	✗	
☐	⇄	Recon task 1	Reconciliation	Closed	HR		closed at 2/11/20, 5:28:47 PM		Show progress	✓	
☐	⇄	Reconciliation (LDAP Resource)	Reconciliation	Waiting	Localhost OpenLDAP				Show progress	✓	

Evolveum

Basic

Task name	
Type:	Choose One
Applicable to type	Choose One
Resource reference	Choose One
Kind	Choose One
Intent	
Object class	
Run only until node down	

Advanced option

Create in SUSPENDED state	
Thread stop action	Choose One
Misfire action	Execute immediately

Options Dry run

Back Save

Scheduling

For one-time tasks, enter neither schedule interval nor cron-like specification. For recurring tasks, enter exactly one of these.

Recurring task				
Do not start before		:		AM
Do not start after		:		AM

Evolveum

Live Sync: LDAP Server (OpenLDAP)

Progress: 876
Last object processed: uid=jan,ou=People,dc=example,dc=com
Started 2/16/20 11:00:49 PM (00:00:02.942 ago)

Running
Success
Refreshing each 2 sec

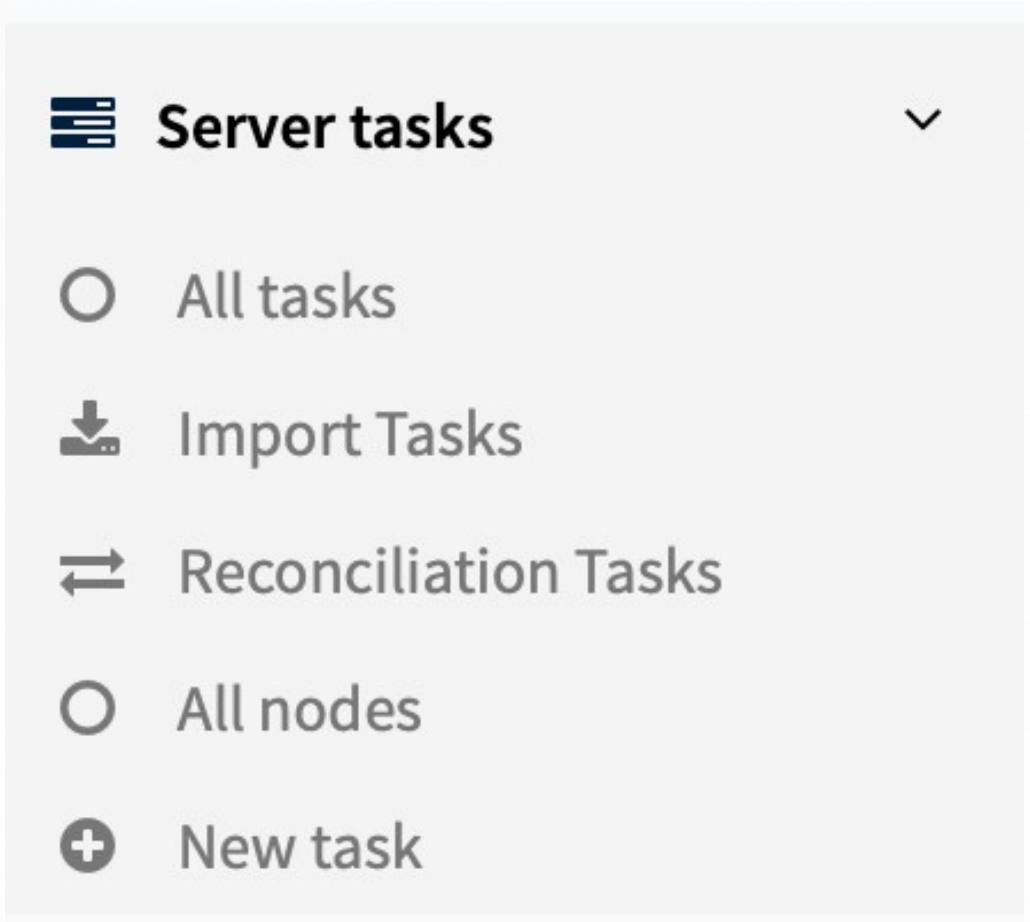
Basic | Scheduling | Progress | Environmental performance | Result | Errors

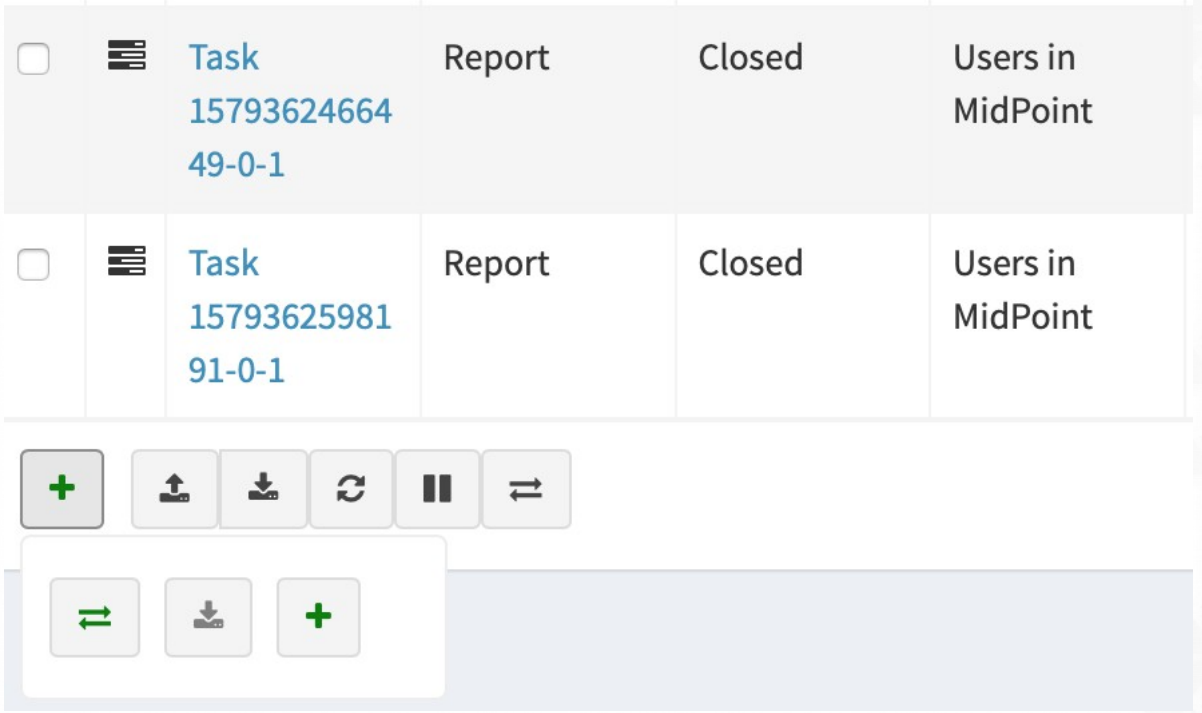
Task name	Live Sync: LDAP Server (OpenLDAP)
Description	Definition of a live sychnronization task. It will poll changelog and pull in changes
OID	87843d58-76b8-11e2-ae3e-001e8c717e5b
Identifier	91919191-76e0-59e2-86d6-3d4f02d3ffff
Category	Live synchronization
Parent task	
Task owner	administrator
Handler URI	http://midpoint.evolveum.com/xml/ns/p sync/handler-3
Execution status	Running - at node DefaultNode

Resource reference	LDAP Server (OpenLDAP) over new LDA
Kind	Account
Intent	
Object class	
Options	Dry run
Synchronization token	20200216220049Z
Retry unhandled errors	

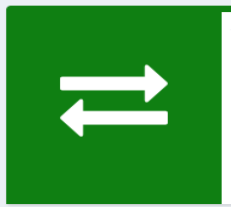
Evolveum

Task Pages





Evolveum



Reconciliation (LDAP Resource)

Progress: 1 (waiting)

2/11/20, 3:33:39 PM - 2/11/20, 3:33:39 PM (00:00:00.454)

Waiting

Success

Reconciliation Task

(no refreshing)

Basic | Schedule | Work management | Cleanup policies | Subtasks | Operation statistics | pageTask.environmentalPerformance.title | Internal performance | Result | Errors

Properties

Resource related options

Object	Edit — Localhost OpenLDAP: ResourceType
objectclass	inetOrgPerson
kind	Account
intent	default

Show empty fields

Advanced options

Operational attributes

AD Connector Without Powershell

```
<connectorConfiguration>
<icfc:configurationProperties>
    .....
    <icfcldap:winRmUsername>midpoint</icfcldap:winRmUsername>
    <icfcldap:winRmDomain>midpoint</icfcldap:winRmDomain>
    <icfcldap:winRmAuthenticationScheme>credssp</icfcldap:winRmAuthenticationScheme>
    <icfcldap:winRmPort>5986</icfcldap:winRmPort>
    <icfcldap:winRmUseHttps>true</icfcldap:winRmUseHttps>
    <icfcldap:powershellArgumentStyle>variables</icfcldap:powershellArgumentStyle>
</icfc:configurationProperties>
<icfc:resultsHandlerConfiguration>
    ...
</icfc:resultsHandlerConfiguration>
```

Evolveum

AD Connector Without Powershell

```
<additionalConnector>
    <name>powershell</name>
    <connectorRef>
        <filter>
            <q:equal>
                <q:path>c:connectorType</q:path>
                <q:value>com.evolveum.polygon.connector.powershell.PowerShellConnector</q:value>
            </q:equal>
        </filter>
    </connectorRef>
    <connectorConfiguration>
        <icfc:configurationProperties>
            ....
        </icfc:configurationProperties>
        <icfc:resultsHandlerConfiguration>
            ....
        </icfc:resultsHandlerConfiguration>
    </connectorConfiguration>
</additionalConnector>
```

Evolveum

Be careful what you wish for
–
you may get it

Evolveum

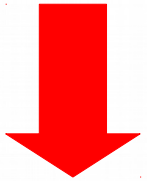
Planning Yesterday

- 2011 – 2014
  - Self planing
  - Easy life
  - (Almost) no customers, no problem, no money
- Since 2015
  - Customer driven approach
  - No milestones
  - New feature request during any phase

Evolveum

MidPoint 4.0

- Big deployments, big problems
- (almost) Every week new feature request
- New features 2 days before release
- No milestones, no specific dates, rough estimates (April, October)



- Delay half a year
- Stability and robustness suffered

Evolveum

Planning Today

- Milestones
  - 30 working days (excluding public vacations)
  - Specific dates
- Features planned for specific milestones
  - More complex features at the beginning
- Freezing scope
  - Not perfect, still some feature request during development cycle
- Estimates based on real (past) data

Evolveum

Planning Tomorrow

- Fixed time

  Exact dates for Milestones, Release, ...

- Fixed people

  New people are not effective from Day 1.

- Fixed max scope

  Some features might be shifted

Evolveum

Thank you for your time

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

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

 /Evolveum

 /Evolveum

 /Evolveum

 @Evolveum

 /Evolveum

Evolveum