



2nd Annual MidPoint Community Meetup

Manual Connector Development

Evolveum



Funded by the
European Union
NextGenerationEU

**[RECOVERY
AND RESILIENCE]
PLAN**

Matúš Macík, May 2026
Senior IAM Engineer

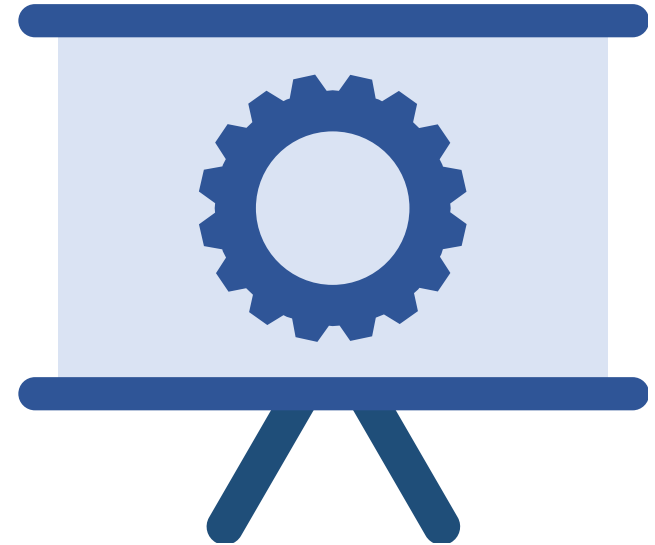
Agenda

- **What are manual resources ?**
- **Why should we care** about them ?
- **How** can we **manage** them?
- **What** are **manual connectors**?
- **How** can I **implement** one?



What Are Manual Resources?

- **Offline resources** requiring **manual** action
 - **Not connected** to midPoint via an **Identity Connector**
 - **Provisioning** not possible or **lacking API**
 - **Legacy, externally managed, highly restricted**
- **Manual Provisioning**
 - **Tickets** are created for **system Administrators**
- **Connectors**
 - “**Build In**” **Manual Connector**
 - **ITSM integration** through the “**Manual Connector**”



Why do we have this approach ?

- Don't exclude "offline" resources
- Keep the **same governance workflow**
 - Use **midPoint** to manage access
 - **Keep track**, keep audit trails and consistent state
- Not fully **automated**, yet still **governed systems**
 - **Policy enforcement, accountability and tracked lifecycle**



Manual Resource Workflow

- HR triggers role assignment
- MidPoint determines required **account & attributes**
- Creates **ticket** for admin (in the ITSM system)
- **Administrator** manually **executes operation**
- **Ticket closed** and **midPoint updates** cached **account data**
- All **changes** are **stored** as **deltas in repository** during execution



Data consistency

- **Pure manual resources** have **no direct feedback** from target system
- **Cached data** is only midPoint's "**estimate**" of account state
- **Target system changes unknown** to midPoint
- **Visibility problem**, we need to bridge



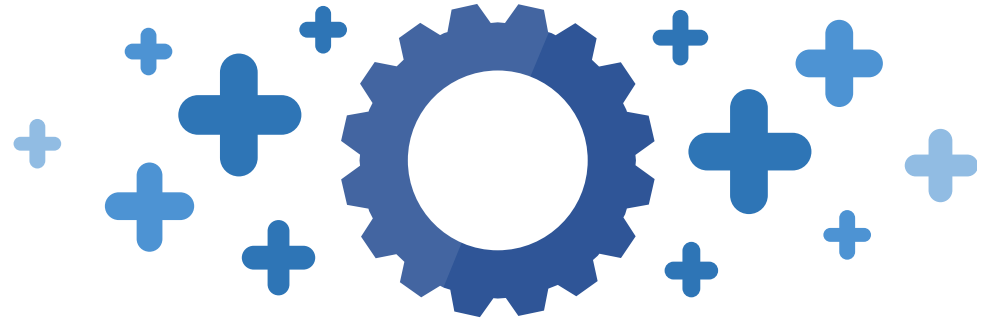
Semi-Manual Resources

- **Combination** of a **manual connector** and an **ordinary connector**
 - **Manual connector: Provisioning ops** (create/update/delete)
 - **Online connector: Read operations** (e.g., CSV export, database, REST read)
- **Merges operation deltas with last-known state**
- **Detects illegal changes** on target system
- **Validates admin execution** & auto-creates **remediation tickets**



Multi-Connector Architecture (Manual Resources)

- **One primary** connector (**Manual Connector**)
- **Additional connectors**
- **Same schema for all connectors**
 - **Originating from one of the “Additional Connectors”**
- **Each operation routed to single connector**
 - **For others the operations are disabled**



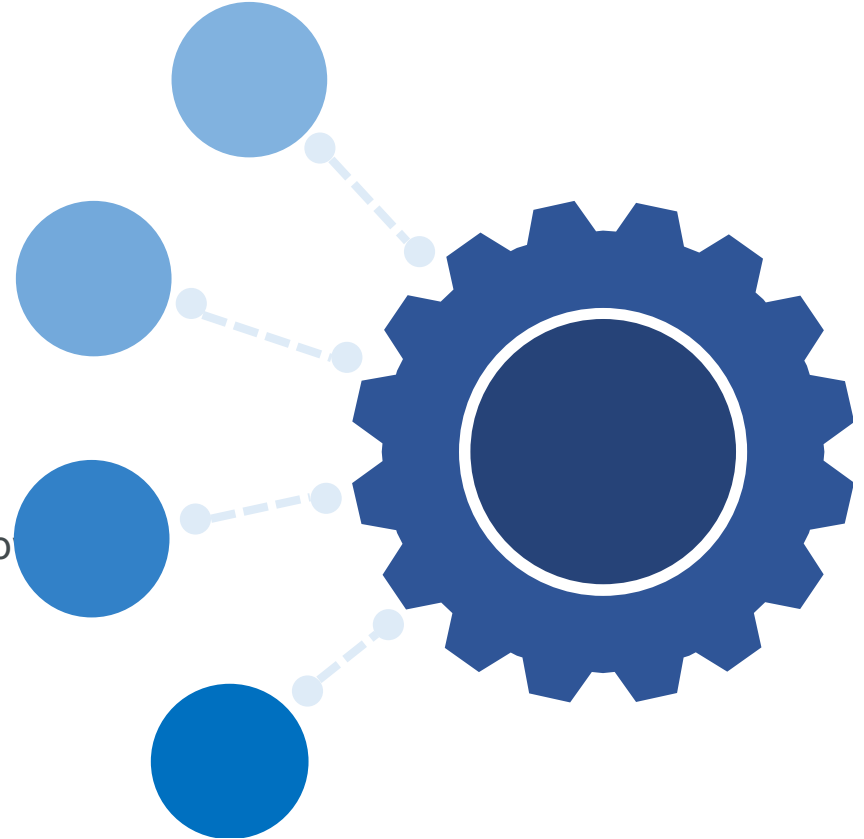
Internal Provisioning Cases

- **MidPoint** has **built-in case management** (similar to ITSM tickets)
- **Tighter integration** with identity data
- **Use for:** Identity **governance, compliance, policy violation** tracking
- **Alternative to external ITSM if not integrated**



Manual Resource Management

- **Pure build in manual connector**
 - Leveraging the build in workflow engine
- **Integration with existing ITSM systems** (Jira, ServiceNow, Remedy, etc.)
 - Admins work with **familiar ITSM interface**



Legacy approach to Manual Connectors (ITSM plug-ins)

- Usage of the **Unified Connector Framework (UCF)**
 - **Specialized connectors** (manual, built-in)
 - **Manual connectors** extend **AbstractManualConnectorInstance**
 - Have the **@ManagedConnector** annotation
- **No external OSGI/JARs** (embedded in midPoint)
- **Explicitly** must be **built together with midPoint**



The Current Approach, ITSM Connectors

- Rather than **plugins**, implement **connectors** for **ITSM systems**
 - SCIMREST or pure conId
 - Implementation **same** “as usual”
 - MidPoint needs to “**create**” and “**read**” tickets
 - Ticket has it’s own **schema** and **own lifecycle**



The Current Approach, ITSM Resource

- **ITSM resource** object
 - Represents the **ITSM system**
 - **Schema** of the **ticket/cases**
 - Mappings and object classes linked to caseType
- The **Manual resource** object
 - Represents the “**target system**”
 - **Schema** of the **object on the target system**
 - **Configuration** references the **ITSM Resource**



The workflow with ITSM connectors

- **Change in User results in**
 - Manual resource **constructs a case (on MidPoint)**
 - Manual resource **links it to the ITSM Resource**
- **The ITSM resource**
 - **Creates a Ticket**
 - **Handles it's lifecycle**



Provisioning Propagation

- By default **changes** are **executed immediately**
 - Best for **quick, efficient** “on-line” **resources**
- **Propagation** configuration and task
 - When **operations** are **slow** and **expensive**
 - **Changes** are **queued** for **some time** (**pending deltas** in shadows)
 - **Changes** will be **executed in a single operation**
 - All the **pending changes** in the **shadow**
 - **Resource configuration** and **Task**
 - Shadows with **pending deltas older** than the **specified interval**



Grace Period

- **Finished pending operation** information (deltas) is **deleted by default**
- **Retain deltas during the “Grace period”**
 - **Inspection** of the **operation status/ outcome**
 - **Latency** of **semi-manual** resources
- **During the grace period**
 - **Deltas applied** and **new deltas** are **computed on top of them**
 - **Read** returns **“the data the way it should be”**
- **After it expires**
 - **No pretending** any more
 - **Reconciliation** **re-tries the operation** if not applied



Conclusion

- Evolveum **Docs**
- Evolveum **Github**
- Any connector **contributions** are welcome



Evolveum

Thank you for your attention

Feel free to ask your questions now!



Funded by the
European Union
NextGenerationEU

**RECOVERY
AND RESILIENCE
PLAN**



2nd Annual
MidPoint Community Meetup