2nd Annual

MidPoint Community Meetup

# Governance of Non-Human Identities

Slávek Licehammer, May 2026
Head of Engineering

Evolveum

# Agenda

- Introduction to Non-Human Identities (NHI)
- Governance of NHI
- NHI in midPoint
- Conclusion and recommendation

# From Human to Non-Human Identities (NHI)?

- Human identities are prime
- NHI are naturally occurring
- Modern IT is mostly automatized
- Blurring the differences
  - Devices, services, agents acting as a user
- Zero trust principles
- Embrace non-human identities

# Why Non-Human Identities?

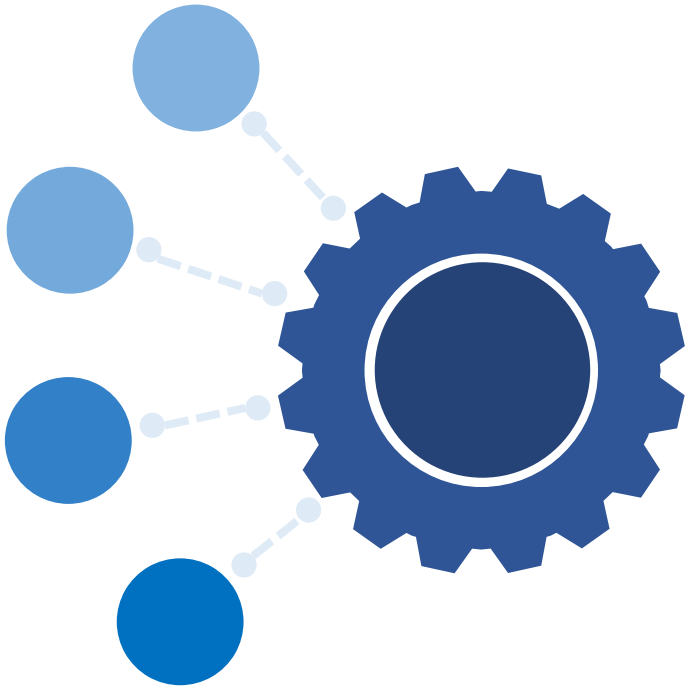
- The number is rising
  - Estimates are 20-50x more than human identities
- Often overlooked
  - Both life-cycle and usage
- Huge potential attack surface
  - Privileged by design
- Harder to manage
  - Scale
  - Shared ownership

# Types of Non-Human Identities

- Service accounts, system accounts
- Devices
- Internet of things
- Applications, micro-services
- Agents, bots
- Integration code, CI/CD
- Workload
- ...

# Typical Approach to Non-Human Identities

- Low-level approach to NHI management
- Security
- Credential management
- API protection
- Monitoring, risk assessment
- There are many specialized solutions for it

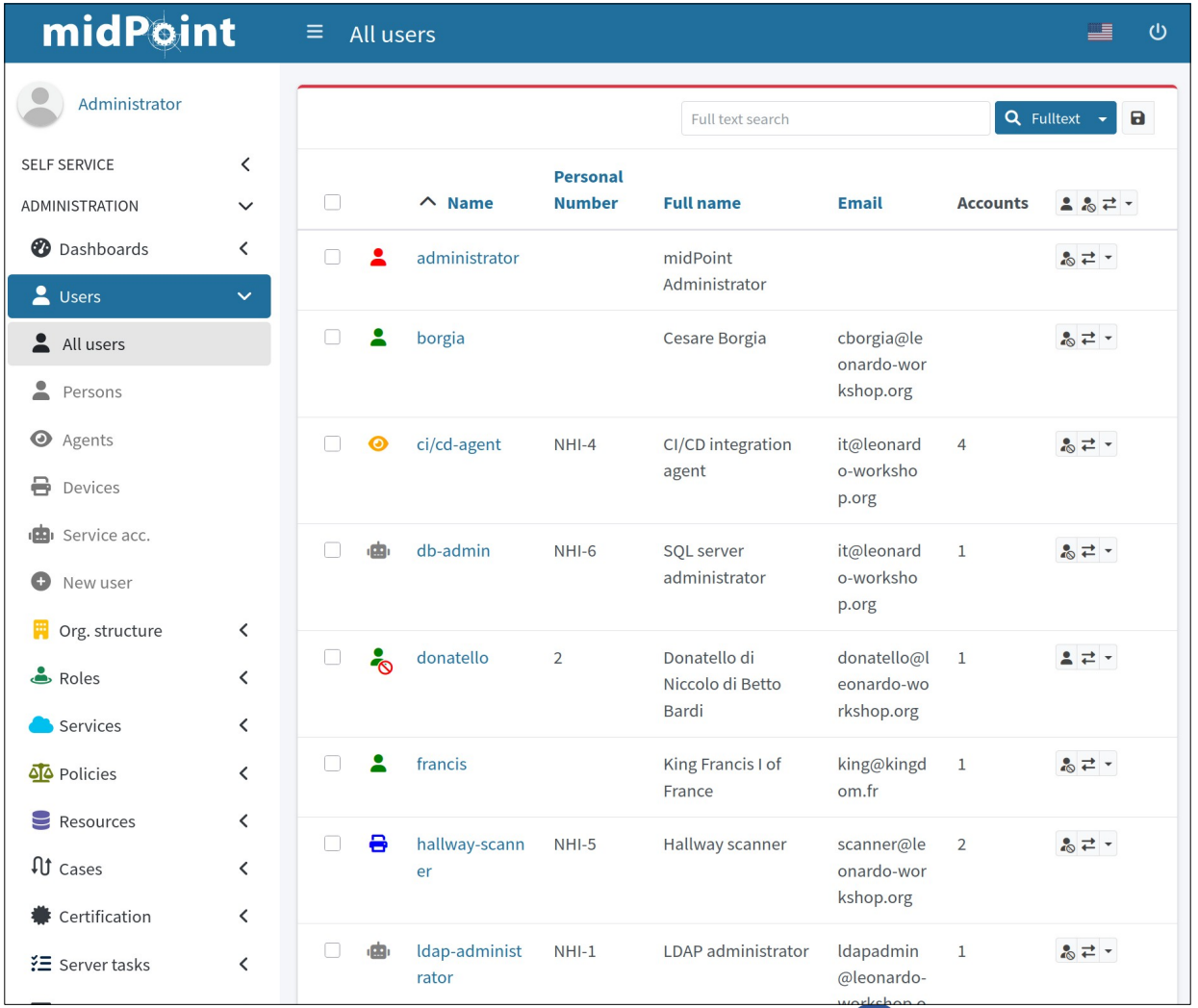


# What About Governance?

- Governance as an essence of managing NHI
- A high-level approach to NHI governance
- Why does NHI exist? (purpose)
- Who is responsible? (ownership)
- What can NHI do? (authorization)

# Modeling NHI in midPoint

- Service object
- Use archetypes
  - Different types of NHI
- Track ownership
  - Users, org. units
- Manage life cycle
- RBAC




Evolveum

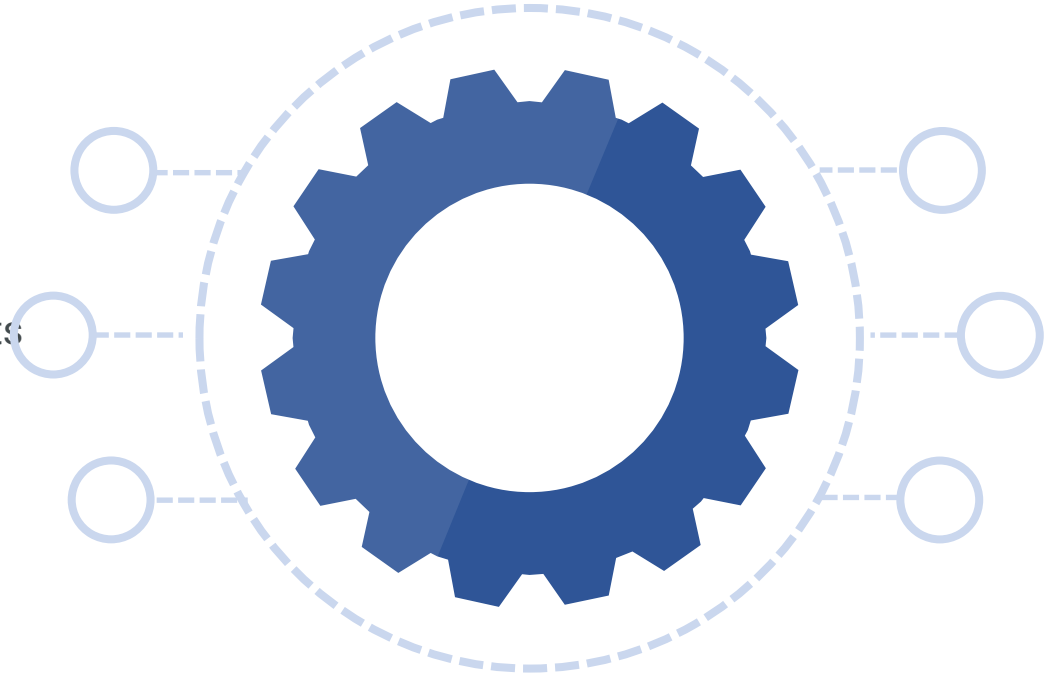
2nd Annual MidPoint Community Meetup

# Lifecycle

- Standards lifecycle options
  - Manual management in midPoint
  - External source
- Approvals for creation and new accesses
- Lifecycle based on ownership
- Recertification of ownership

# Discovery & Provisioning

- Using standard connectors
  - Use different kind / intent
- Manage accounts for access management
- Consider reaction on newly discovered accounts
  - Report
  - Disable
- Integrate with other NHI management tool
  - Make sure are accounts are managed



# Conclusion

- Existing IGA principles are applicable to NHI
- You most likely have an IGA or IdM
- You can start by extending the existing IGA with NHI
  - Minimal initial investment
- Then you can continue with specialized tools or by extending NHI-related IGA processes
- **It is recommended to start with inventorization & ownership responsibility**


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