Governing Non-Human Identities with Proven IGA Principles

Slávek Licehammer, May 2025
Head of Engineering

Agenda

- Introduction to non-human identities (NHI)
- Management of NHI
- Governance of NHI
- Conclusion and recommendation

Evolveum

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

Evolveum

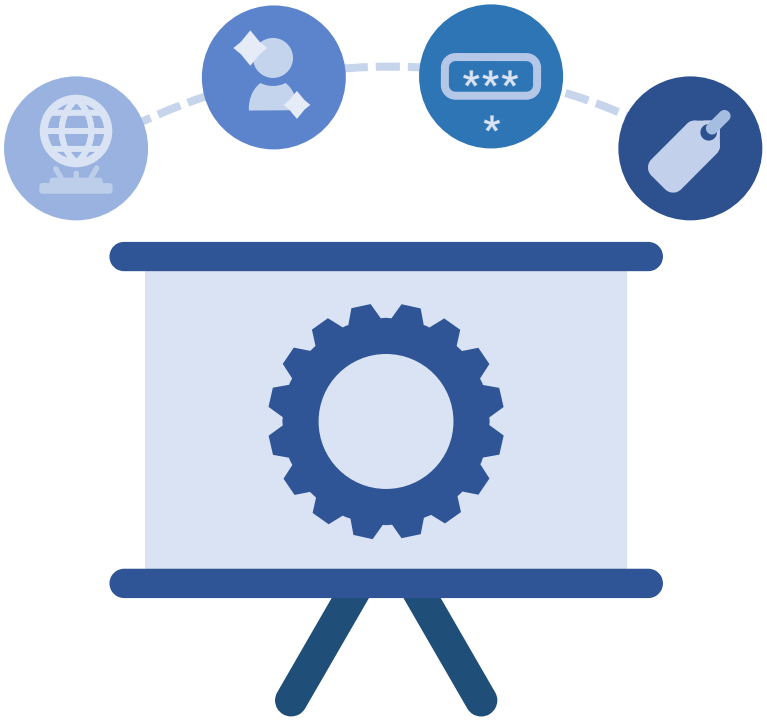
Why Non-Human Identities?

- 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

Evolveum

Types of Non-Human Identities

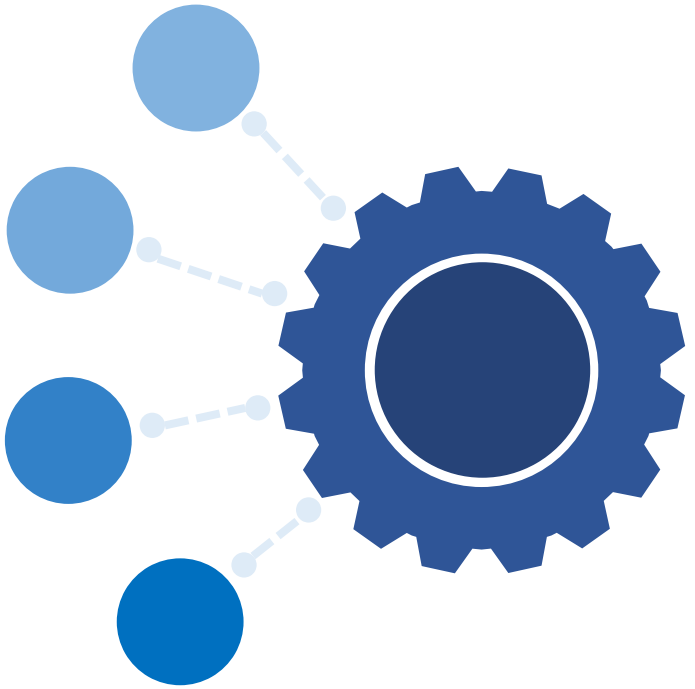
- Service accounts, system accounts
- Devices
- Internet of things
- Applications, micro-services
- Agents, bots
- Integration code, CI/CD
- Workload
- ...



Evolveum

Typical Approach to Non-Human Identities

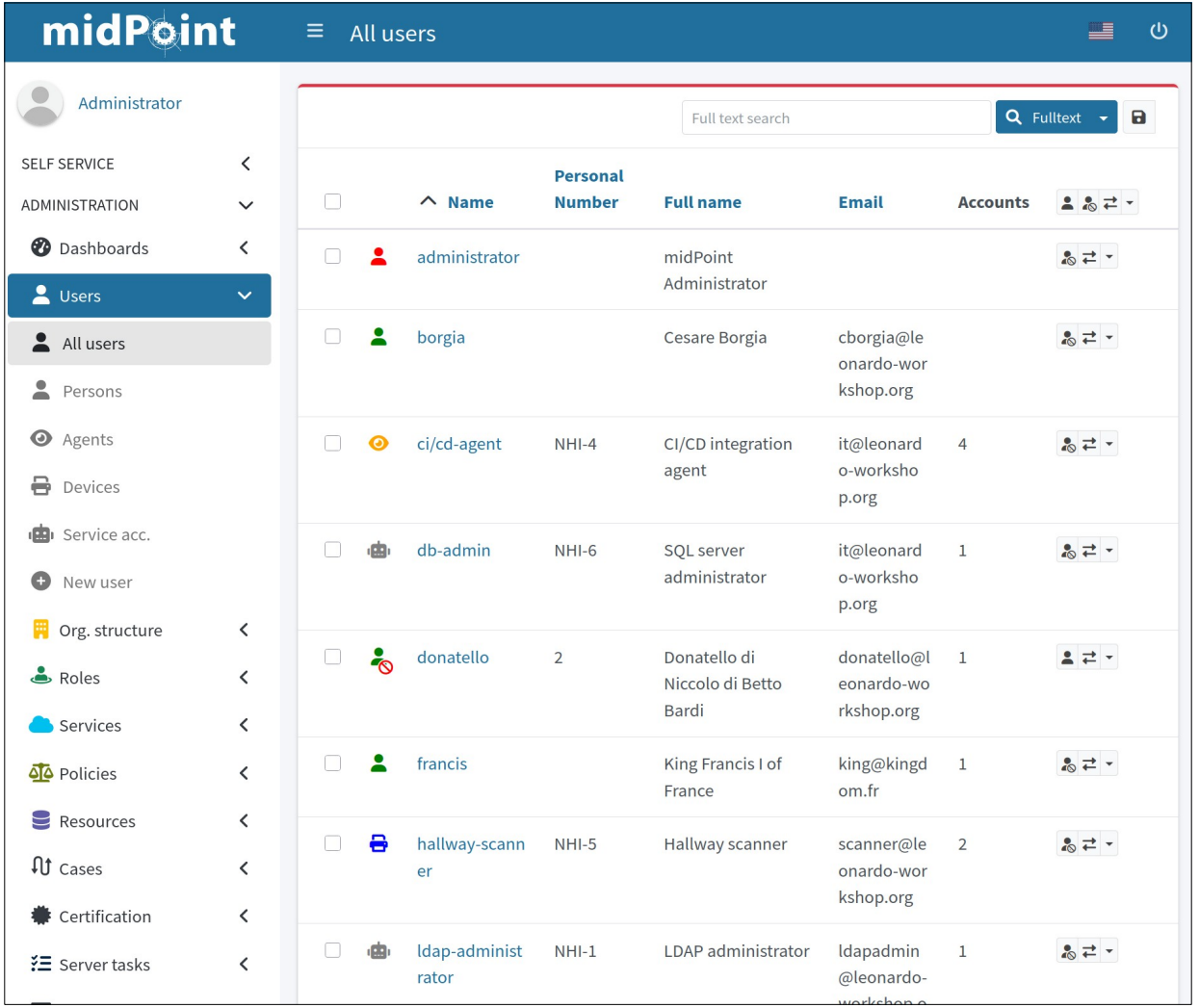
- Low-level approach to NHI management
- Security
- Credential management
- API protection
- Monitoring, risk assessment
- There are many specialized solutions for it



Evolveum

A Different View of NHI

- Evolveum focuses on IGA
- MidPoint
- Open source IGA platform made in EU
- Thinking about NHI from the IGA point of view



Evolveum

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)

Evolveum

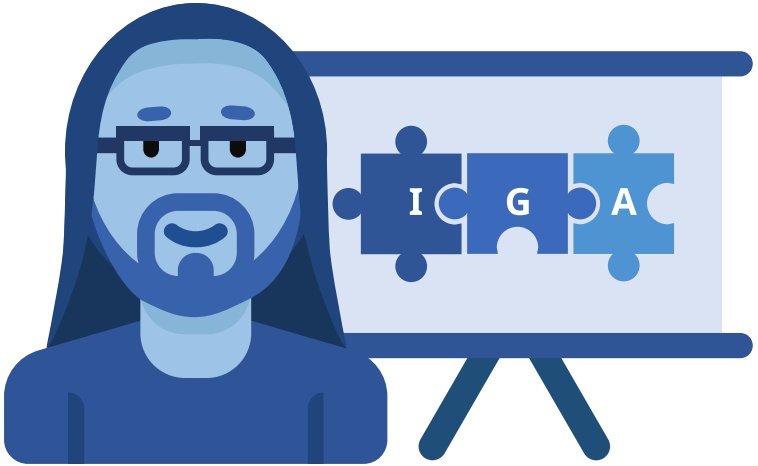
Governance Principles Applicable to NHI

- Life-cycle management
- Approvals
- Access certifications
- Auditing
- Notifications
- Reporting
- Outlier detection
- Risk assessment

Evolveum

Evolveum's View on NHI Governance

- Existing IGA principles are applicable to NHI
- Inventorization / catalogization
- Ownership management
  - React to ownership change
- Management using connectors
  - Expensive
  - Enables discovery, usage monitoring...
- Manage "master" identities for short lived ones
- Integration with specialized tools



Evolveum

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

Do you have any **questions**? Feel free to contact us at **info@evolveum.com**

Meet me and the Evolveum team at **booth #52**

 /Evolveum

 @Evolveum

 /Evolveum

 /Evolveum

 /Evolveum

Evolveum