Dead Ends in Identity Management

2025

Radovan Semančík

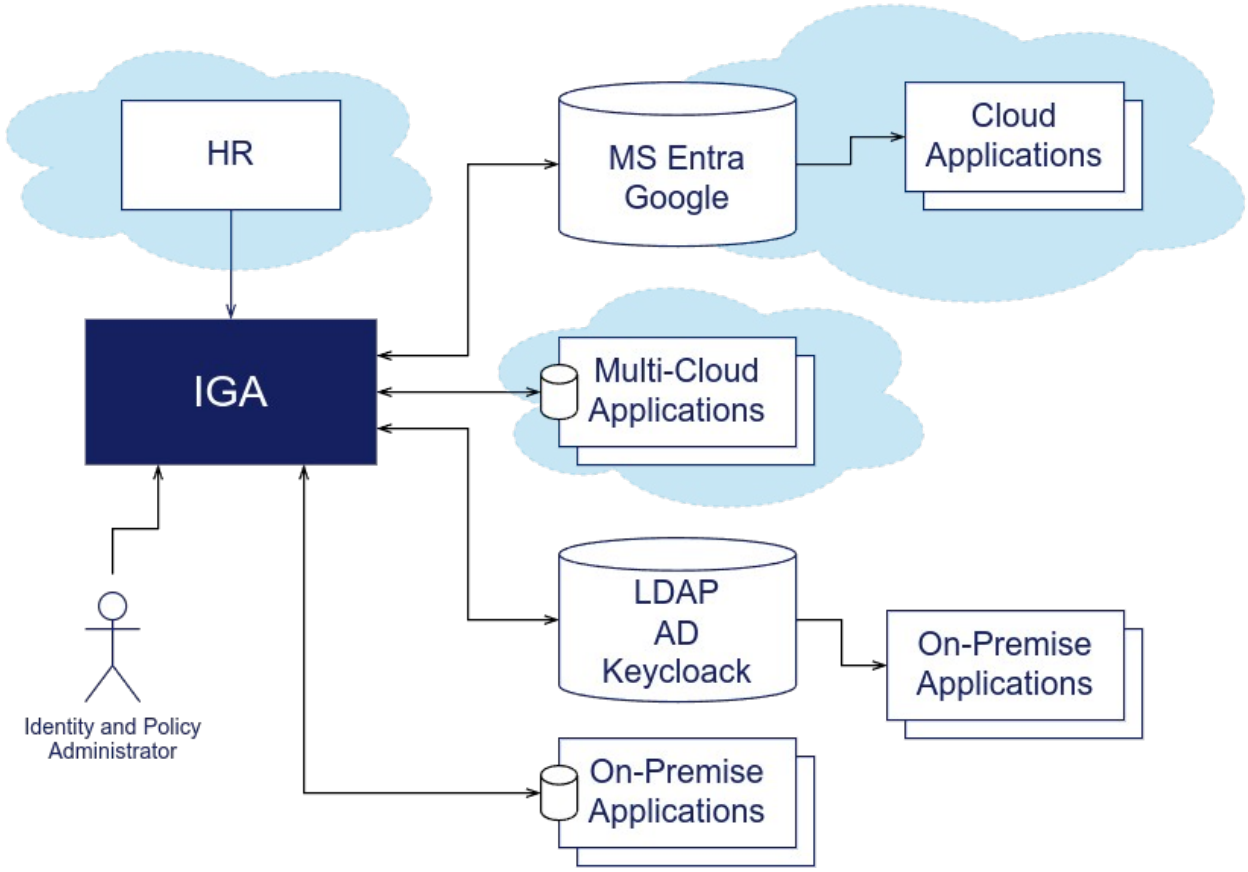
Ing. Radovan Semančík, PhD

- Software Architect at **Evolveum**
- Architect of **midPoint** identity platform
- **Open source** professional
- **Identity** practitioner since early 2000s
- Retired **Apachee Foundation** committer

/semancik @semancik.bsky.social /semancik

Identity Management and Governance

- It is **not** authentication
- Identity **inventory**
- Identity **lifecycle**
- Access control **policies**
- Governance = **high-level policies**
- **Responsibilities** (e.g. owners)
- IGA: Identity Governance and Administration
- Often (shamefully) neglected



If you do not have identity governance, you have no cybersecurity.

Cybersecurity is all about users - their actions, permissions, the value they create and the risk they are posing. If you do not control the users, you control nothing. All your cybersecurity is just an illusion.

Dead Ends / Antipatterns / Bad Practice / Myths

- Simple, easy to understand and *wrong*
- Identity can be very *counter-intuitive*
- Dead ends: based on more than two decades of IAM experience
  + experience from development and use of midPoint

Big Bang

My Data Are Perfect

AI Will Fix It

IAM Is Authentication

IGA Is Access Control

Policies Are Easy

Identity Project

RBAC Is Dead

Access Review Obsession

First Steps In Identity

- Usual start: **authentication** **[WRONG]**

  Strong authentication of *unmanaged* accounts => vulnerability

First Steps In Identity

- Usual start: **authentication** **[WRONG]**

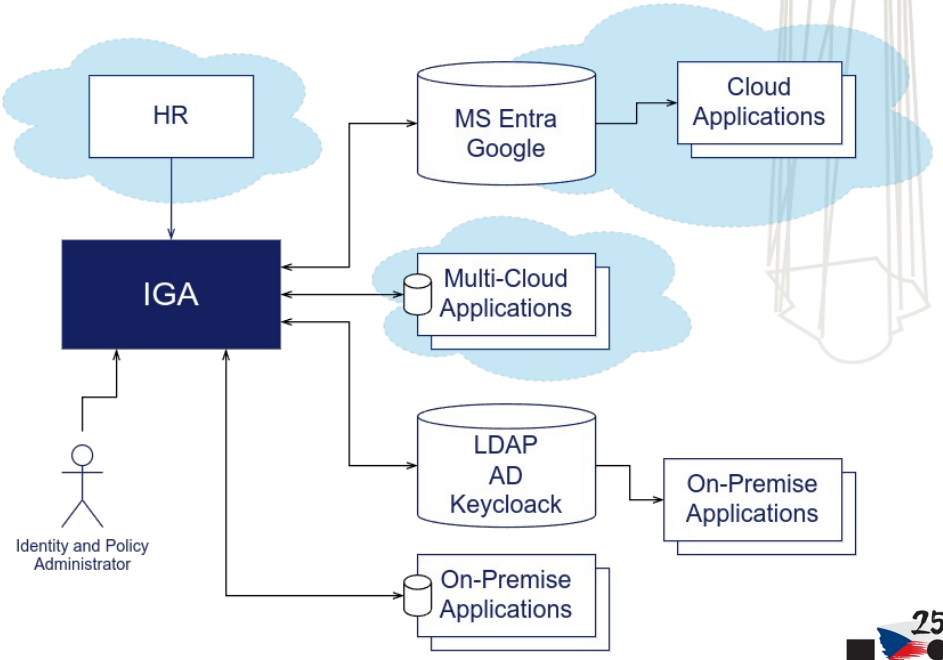
  Strong authentication of *unmanaged* accounts => vulnerability

- Identity cannot be an afterthought

- Start with **management**: **[CORRECT]**
  inventory, ownership, lifecyle,
  detect orphaned accounts

- **Recommendation**:

  Start your IGA effort early.
  It may be „light“ IGA, yet it is necessary.



My Data Are Perfect

- Usual start: Raw HR data **[WARNING]**

  Data never cross-checked => low quality

My Data Are Perfect

- Usual start: Raw HR data **[WARNING]**

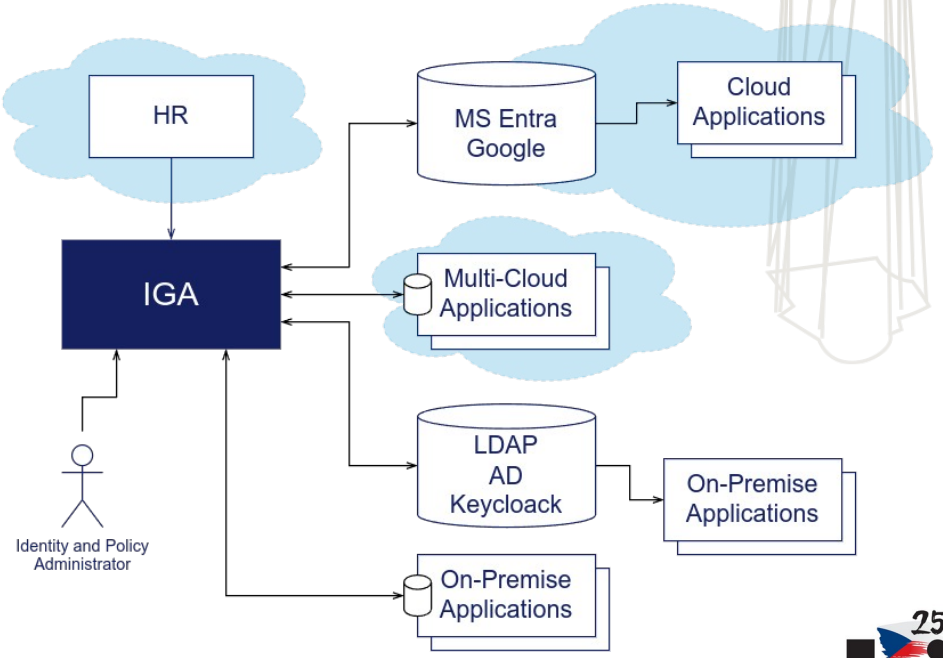
  Data never cross-checked => low quality

- Data quality is critical for policies and automation

- Clean up the data before use: **[CORRECT]**
  synchronization, correlation, linking

- **Recommendation**:

  Cortelate and compare source data (HR) with target systems (AD, Entra) to clean up data.



Identity Project

- Identity as a **project** **[WRONG]**

  Big bang, fixed scope, fixed deadline => failure

Identity Project

- Identity as a **project** **[WRONG]**
  Big bang, fixed scope, fixed deadline => failure
- Identity effort never ends
- Identity is a **program**: **[CORRECT]**
  iterative and incremental
- **Recommendation**:
  Start small, proceed in increments.
  Create sustainable program.

Access Control

- Policies are easy! **[WRONG]**

  RBAC is dead, we need to use ABAC/PBAC => huge complexities

Access Control

- Policies are easy! **[WRONG]**

  RBAC is dead, we need to use ABAC/PBAC => huge complexities

- Policy is complex, and usually not completely known

- Righ tool for the job: **[CORRECT]**
  regular access → algorithmic ABAC/PBAC
  irregular access → dynamic RBAC
  handling of policy exceptions

- **Recommendation**:

  Bottom-up approach: build roles/policies from current state.

Governance vs Management

- We set up policies and we are done. **[WRONG]**

  Policies without proper maintenance => policy rot

Governance vs Management

- We set up policies and we are done. **[WRONG]**
  Policies without proper maintenance => policy rot

- Everything needs care and maintenance

- Governance is all about **responsibility**: **[CORRECT]**
  inventory, ownership, classification, review

- **Recommendation**:
  Set up high-level policies to watch over governance.
  (e.g. checking that every application has an owner)

Acess Review Obsession

- Reduce access using access review **[WRONG]**

  Massive access review campaigns => huge effort, small effect

Acess Review Obsession

- Reduce access using access review **[WRONG]**

  Massive access review campaigns => huge effort, small effect

- Review fatigue, rubber-stamping

- Policies and automation over reviews **[CORRECT]**

- **Recommendation**:

  Focused campaigns: risk, privileged access.
  Prefer micro-certifications (micro-reviews).
  Bottom-up approach to create policies.

Artificial Intelligence Will Fix It All

- AI will do all the things that we cannot **[WRONG]**

  Over-reliance on AI => your bad decisions get entrenched

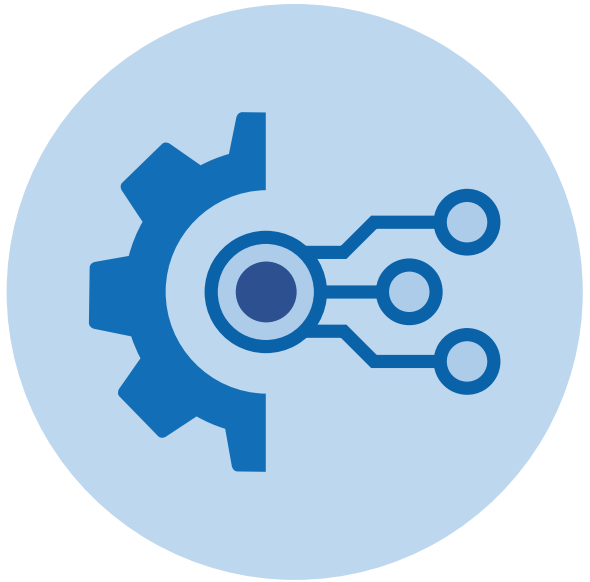
Artificial Intelligence Will Fix It All

- AI will do all the things that we cannot **[WRONG]**
  Over-reliance on AI => your bad decisions get entrenched

- Nobody knows how your policies *should* look like

- Human expertise is still essential **[CORRECT]**
  AI can make human experts more efficient

- **Recommendation**:
  Keep human expert in the loop.
  Start with proven techniques: role mining, outliers.
  Require *explainability* of AI-based recommendations.



Conclusion

- Identity management & governance is necessary for cybersecurity

  … yet, it can be confusing

- Identity myths

  https://docs.evolveum.com/iam/myths/

- Key recommendation: iterative approach

/semancik @semancik.bsky.social /semancik