

Slavek Licehammer / December 2022

MidPoint

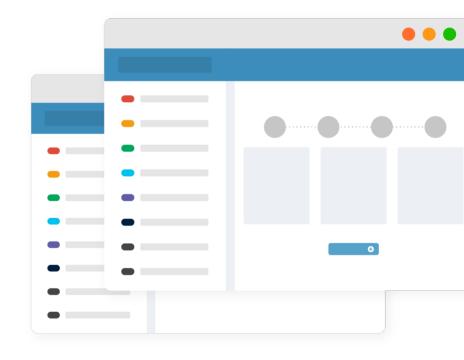
- Open source IdM and IGA platform
- Flexible and customizable solution
- Strongly influenced by academia
- One of Trusted Access Platform components

	X SCAL	LABILITY			John Smith (jsmith) Programmer			PRIVACY-ENHANCING IDENTITY MANAGEME	
	Name				▼ Proper	rties ≭ ∔≙ ©		Privacy protection	
	johnd			= •					
	•			2 -	Full nar	me John Smith		Levels of assurance	
_	i —	USERS			Positio	n Trainee			•
			.000 enabled						
		oo total			_				
	•		-	# +	_	_			
	• -		-	# ·					
	i —			= -	_				
	E MAN					E IDENTITY		ADDRESSING REGULATIONS	
		IAGEMEN		M S`	IULTIPL YNCHR	E IDENTITY ONIZATION CORRELATIO		REGULATIONS AND COMPLIANC	æ
LICENS	e Name T	IAGEMEN		M S`	IULTIPL YNCHR MART (ONIZATION		REGULATIONS	æ
LICENS License Q AD Azur	e Name T	IAGEMEN	IT	M S`	ULTIPL YNCHR MART (N	REGULATIONS AND COMPLIANC	æ
LICENS License Q AD Azur	e Name T	IAGEMEN Type E5 Developer Peck	IT ⊚≓∙	M S`	IULTIPL YNCHR MART (ONIZATION		REGULATIONS AND COMPLIANC 84.24% compliant data protection policy Wate Vite	
License Q AD Azur Q Google 1	e Name T re E Workspace B	IAGEMEN Type E5 Developer Peck	IT	M S`	IULTIPL YNCHR MART (Name @	ONIZATION CORRELATIO Resource 0 HR	v g •	REGULATIONS AND COMPLIANC	
License AD Azur Google 1 Coogle 1	e Name T re E Workspace B	Type ES Developer Pack Business Plus	IT	M S`	Name 0	CORRELATION Resource • HR LDAP		REGULATIONS AND COMPLIANC 84.24% compliant data potentian poly text sin #	
License AD Azur Google 1 Google 1 Coogle 1	e Name T re E Workspace B	Type ES Developer Pack Business Plus	IT و = • و = • و = •	M S`	Name e Jdoe Jdoe Jdoe	Resource • HR LDAP Canteen Card		REGULATIONS AND COMPLIANC 84.24% compliant data point war with 0 objects in violation security picture war with	
License AD Azur Google 1 Google 1 Coogle 1	e Name T re E Workspace B	Type ES Developer Pack Business Plus	T	M S`	Name e Jdoe Jdoe Jdoe	Resource • HR LDAP Canteen Card		REGULATIONS AND COMPLIANC 84.24%, compliant data patherida paloy war wa	



MidPoint - News

- GUI improvements
 - Customization
- Smart correlation
 - ID Match integration
- Open ID Connect support
- Axiom query language improvement
- Request access wizard
- Resource definition wizard
- Better containers and Kubernetes support



IGA Identity Governance and Administration



- Focus on "business" users
 - Shift from engineers
- Visibility
- Delegation of responsibilities
- Processes
- Automation
- Security





Motivation

- Empower users
- Remove burden from technical staff
- Speed up organizational processes
- Maintain order
- Reduce costs
- Digital transformation



Evolveum

Motivation

- Empower users
- Remove burden from technical staff
- Speed up organizational processes
- Maintain order
- Reduce costs
- Digital transformation







- Visibility
 - For non-technical users
 - Reports, audits
 - Risk analysis
- Policies
 - Security
 - Automation
 - Compliance





Visibility

- "Who has access where and why"
- Understanding for non-technical users
 - Understanding own accesses
- Business, technical, application roles
- Concept of application
 - Member of AD Group vs access to WiFi
- Manual access rights management
 - Utilization of organizational structure



Reporting, Dashboards

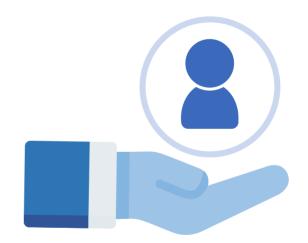
- Overview on any level
- Easier debugging, monitoring
 - Notifications
- Audits
- Security
- Compliance
- Risk analysis



Evolveum

Role Request

- Self-service
- Fast and easy
- Empower end users
- User understand what role is needed
- Combination with other processes
 - Approvals, certification, expiration
 - Role mining



Role Engineering

- Preparing roles for role request
- Requires application and IdM experts
- Long term process (day)
- Can be automated
 - Application inventory
- Separate it from role assignments/requests





Approvals

- Approval for selected actions
 - Triggered by self service
 - Triggered by other events (e.g. adding user to role or group)
- Multistage approvals
- Deputies
- Escalation
- Don't overuse it
 - Notification



Evolveum

Access Certification

- Check manually added rights
- Crucial for maintaining order
- Scheduled campaign
- Lightweight process
 - Easy for reviewers







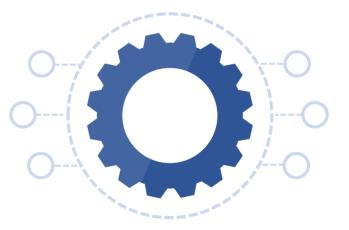
- Enforce policies within IdM
 - Segregation of duties, approvals, compliance, lifecycles
- Reporting
- Policy remediation
- Compliance
- Risk analysis





Global Integration and Processes

- MidPoint can work with any identity object
 - Objects/identities are created outside IGA
 - IGA responsible for: relations, rights
- Application catalog
- Identity of devices
- Entitlement management
- Organization wide workflows



Where Are We With MidPoint?

- Focusing on visibility
- Self-service done
- Approvals done
- Access certification done
- Policies partialy done
- Processes partially done
- Notifications, reports, dashboards done



Evolveum

Conclusion

- Visibility and policies
 - "Who has access where and why"
- IGA is complex
- IGA bring lot of benefits
- midPoint is IGA platform
- New IGA-related features in midPoint 4.7





Thank you for attention

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

Also follow us on our social media for further information!



