How to Govern and Maintain Compliance Using Open Source Identity Management Components

May 17, 2017
ApacheCon NA, Miami
Introductions

• Katarina Valalikova
  – @KValalikova
  – k.valalikova@evolveum.com

• Shawn McKinney
  – @shawnmckinney
  – smckinney@symas.com
Session Objective

The rationale for

Learn about identity governance and demo some common use cases w/ midPoint.
Session Agenda

- Terminology
- Benefits
- Governance
- Architecture
- Demo
- Questions
Terminology

identity

ApacheCon NA, Miami 2017
Terminology

organizational structures
Terminology

<- security policies
Terminology

provisioning ->
Terminology
Terminology

<- IdM System
What can IdM do for you?

1. Too many accounts
2. Too few accounts
3. Have an idea of how many accounts
4. Principle of least privilege
5. Know who did the assignment
Yes, but what about?

1. Sensitive roles not managed properly
2. Too many, too few assigned, i.e. only one can have this role
3. Accounts not properly assigned
4. Managers on leave
5. Adjudication
6. Changes made directly to target system
In other words, we need

1. Access certification
2. Approvals
3. Notifications
4. Escalation
5. Deputy
6. ....
What is Identity Governance?

Gartner says:
• Combines with IAM functions to meet audit and compliance obligations.
What is Identity Governance?

Radovan says:

• High-level business processes, business rules, policies, organizational structures
• Combines with low-level identity management processes like data synchronization, system integration, data formats, data transformation, network protocols
• Radovan Semancik, wiki.evolveum.com
What is Identity Governance?
Role Based Access Control
Role Based Access Control

- **RBAC0**
  - Users, Roles, Perms, Sessions

- **RBAC1**
  - Hierarchical Roles

- **RBAC2**
  - Static SoD

- **RBAC3**
  - Dynamic SoD

ANSI INCITS 359
Identity Management and Governance

BUSINESS

GOVERNANCE

RBAC

IDM

TECHNOLOGY

POLICY

ApacheCon NA, Miami 2017
Solution

midPoint

Apache Software License 2.0
Architectural Overview
Architectural Overview

Requires
• Java version 8
• Java servlet container
• Relational database
  (any)

Uses
• Spring Framework
  – component wiring
• Apache Wicket
  – user interface
• ConnId
  – common connectors
Architectural Overview

User interface components

High-level components don't connect with low-level components

High-level components:
- gui subsystem
- model subsystem

Low-level components:
- repository subsystem
- provisioning subsystem

Customizable and configurable

Data storage and task management

IdM services, security and user-account mappings

Resource and account management

Common data model, libs and low-level utils
Demo
Users & Accounts

midPoint

Active Directory
- Account "aanderson"

Linux
- Account "alice"

CRM
- Account "emp001"
Provisioning

Account: HR
- FNAME: Alice
- LNAME: Anderson
- ID: 001

Account: AD
- dn: cn = Alice Anderson
- cn: Alice Anderson
- givenName: Alice
- sn: Anderson
- telephoneNumber: +421...

Account: CRM
- username: emp001
- name: Alice Anderson
- mail: alice@example.com
Demo Environment

HCM connector (peoplesoft)

Google Apps connector

LDAP Connector
Use Cases

• UC1 – Onboarding
• UC2 - Notifications
• UC3- Approvals
• UC4 - Escalations
• UC5 – Delegations
• UC6 - SoD
• UC7- Certifications
Demo Scenarios

1. Onboarding new emp, account activation
2. Self service, multi-level approval, escalation
3. Role assignment, SoD
4. Deputy
5. Access Certification
1 Onboarding new Identity

1. User is imported from HCM
2. Activation link is sent to the user
3. User activate his account
4. Basic roles are assigned
2 Self service

1. User selects roles he needs to have assigned
2. Request is sent for approval
3. Approval starts
2 Self service

1. User selects roles he needs to have assigned
2. Request is sent to approval
3. Approval starts
4. Approval from security officer is needed
2 Self service

1. User selects roles he needs to have assigned
2. Request is sent to approval
3. Approval starts
4. Approval from security officer is needed
5. Approval from application owner is needed
2 Self service

1. User selects roles he needs to have assigned
2. Request is sent to approval
3. Approval starts
4. Approval from security officer is needed
5. Approval from application owner is needed
6. App owner is on the vacation – escalation
3 Role assignment

1. Manager assigns roles to onboarded user
2. Manager selects conflicting roles
3. Roles are not assigned because of SoD violation
1. Manager is going on vacation
2. Manager delegates his work
5 Access certification

1. New campaign for access certification starts
2. Manager decides which accounts are legal
Benefits of Governance Controls

- Advanced role lifecycle management
- Audit and reporting interfaces
- Enhanced regulatory compliance
- Improved business responsiveness
- Privileged account management
- Self-service interfaces
Governance simply

- Notifications
- Recertification
- (Multi-level) approvals
- Escalation
- Delegation
- Deputy
- Role lifecycle
- Audit trail ...
Questions
Contact

• Katarina Valalikova
  – @KValalikova
  – k.valalikova@evolveum.com

• Shawn McKinney
  – @shawnmckinney
  – smckinney@symas.com