Provisioning and Integration: New Models and Practices

IAM Online – June 12, 2013

Speakers:
- Rob Carter, Duke University
- Jimmy Vuccolo, Penn State
- Jeremy Grieshop, Clemson University

Moderator:
- Keith Hazelton, University of Wisconsin-Madison
Provisioning: An Overview

IAM Online, June 12, 2013

Rob Carter
rob@duke.edu
Provisioning: Three Perspectives

- Authority
  - request
  - create
  - ca. 1985

- System of record
  - System of record
    - Person Registry
      - script
      - ca. 2000
      - create/delete

- System of record
  - populate
  - Provisioning & Integration Tools
    - People
    - Groups
    - Roles/Privileges
    - CIFER (ca. Tomorrow)

Source States
Identity Registries
Consumer States
CONSISTENCY
Provisioning: CIFER Perspective

- CIFER: Provisioning = Processes and integration methods used to establish and subsequently maintain consistency between the states of entities (persons, groups, etc.) in an authoritative source (registry) and various other systems (which may be identity consumers or may be systems of record).

  - Identity states vs. Accounts
  - State Consistency vs. Create/Delete/Replicate
  - Into as well as out of Registries
  - Not just for people anymore – groups, privileges, etc.
But why should I care?
But why should I care?

• Cost containment
  • reduce opportunity cost and manual overhead

• User Experience
  • Users expect “spooky action at a distance” in the social media age
  • “I already told him I moved - don’t you all talk!?!”

• Security
  • Many security issues boil down to poor provisioning & integration
  Inconsistency => confusion => trust failure => breach
But why should I care?

• Cost containment
  • reduce opportunity cost and manual overhead

• User Experience
  • Users expect “spooky action at a distance” in the social media age
  • “I already told him I moved - don’t you all talk!?!?”

• Security
  • Many security issues boil down to poor provisioning & integration

Inconsistency => confusion => trust failure => breach
But why should I care?

• Cost containment
  • reduce opportunity cost and manual overhead

• User Experience
  • Users expect “spooky action at a distance” in the social media age
  • “I already told him I moved - don’t you all even talk?!?”

• Security
  • Weak (de)provisioning & integration cause many incidents
  • Inconsistency => confusion => trust failure or actual breach
Isn’t central authentication enough?

- AuthN = binding a user to an identity
- Provisioning = maintaining the state of identity data in the context where it is used
- Credentials can be provisioned; Authentication may be required to perform provisioning tasks.
Ok, but why now?

- Best of Breed strategies; BYO<whatever>
- Traditional models don’t scale well; vendors are little help
- Cloud Services
  - In the cloud, provisioning may be your only point of control
  - Vendors are as much problem as solution
- Higher Security Reqs
  - Trustees are more security aware now
- Poor provisioning erodes trust both in enterprises and across federations
What’s the solution?

• Good provisioning should exhibit:
  • consistency          • auditability
  • reliability              • scalability
  • flexibility              • integration

• Spectrum of approaches can provide this, depending on needs, resources, capabilities
Provisioning Methods
Use Cases

• Jimmy Vuccolo: Provisioning out of the Penn State Central Person Registry
• Jeremy Grieshop: Bidirectional provisioning to/from ListServ at Clemson
Penn State Use Case

Jimmy Vuccolo, jvuccolo@psu.edu
Manager, Research Programmer
Emerging Technologies
Central Person Registry

A centralized person registry is a single data store that combines and consolidates identity information currently stored in separate and non-integrated sources throughout the University.
Messaging

• Requests the **provisioning** and **de-provisioning** of services.
• Provides **notification** of data changes to registered entities.
Messaging

- Communication between the CPR and service provisioners is accomplished using JMS (Java Messaging Service).
  - Point to point messaging is currently being used.
- Data is encapsulated in a JMS message using JSON (JavaScript Object Notation)
  - JSON represents data using key/value pairs.
Messaging

- Apache’s ActiveMQ provides the messaging infrastructure:
  - Protocols: OpenWire and STOMP.
  - All traffic is SSL encrypted.
  - AuthN/AuthZ on a per queue basis.
CPR Messaging Flow
Anatomy Of A Service Provisioner

• Receives messages from the CPR via JMS.
• Extracts content from embedded JSON.
• Based on command contained within message either provisions, or de-provisions a service.
• Sends results of action back to the CPR.
CommIT Flow

App Servers → CPR DB → Rules

AMQ Broker → Service Provisioner → LDAP
Clemson University

Identity Management and Provisioning

jeremy@clemson.edu, boydw@clemson.edu
IDM Design and Dataflow

Identity Vault and Provisioning Engine

- Self Service UI
- Exchange
- Banner
- Blackboard

Data Filters and Transform Rules

- LDAP
- Mailing Lists
- Unix
Provisioning at Clemson

• Clemson University manages identities for a large number of systems, including: hundreds of Unix systems, Exchange, LDAP, Mailing Lists, Blackboard, Banner, Google, etc.
• In addition to Identity credentials, Clemson provisions associated resources triggered by actions such as enrollments.
• Some systems pull information; some systems push information; and some systems do a combination of both.
Provisioning Model

• Centralized Provisioning Model
  • Tools to house system connection methods
  • Business logic for filtering and transforming data
  • Logging/Auditing in one place

• Notification + Snapshot
  • Unix systems receive instant notification of changes and receive snapshots of User or Group data.

• Changelog Notification
  • Some systems, such as Exchange, receive instant notifications along with the exact data that changed.
Mailing List Use Cases

- Course Sections and enrollments
  - Each academic term automatically alters lists
  - Instructors and Learners are provisioned as List Owners and Members

- Ad-hoc list requests
  - List Owners and Members are manually configured
  - Lists may be changed by central course management tools, or through native Listserv tools.

- Customization support
  - External Members (non-domain users)
  - Custom roles: moderators, quiet owners, etc.
IDM Design and Dataflow

1. Instructor links course sections
2. Student enrolls for Course Section
3. Membership change alters Mailing List
4. BB Resources created for Course Section
5. Admin adds a visiting professor

Self Service UI

Identity Vault and Provisioning Engine

Banner

Blackboard

Mailing Lists
Evaluation
Please complete the evaluation of today’s IAM Online:
http://www.surveymonkey.com/s/IAMOnline_June_2013

Virtual Working Groups – May 20-21
IAM Online has scheduled a special series of virtual working group meetings to showcase key identity and access management tools and services. Grouper, Shibboleth, Social Identity, and more.
https://spaces.internet2.edu/x/NYBHAg
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by Internet2’s InCommon, in cooperation with the EDUCAUSE Identity and Access Management Working Group