Provisioning and De-provisioning Best Practices

Big Ten Academic Alliance Working Group Update

Presented by: Keith Wessel
University of Illinois at Urbana-Champaign
Who are we?

- A working group of the Big Ten Academic Alliance IDM Taskforce
  - The Big Ten Academic Alliance, formerly the CIC
  - A consortium of the Big Ten schools plus U. of Chicago
- Also a TIER working group
Why Provisioning?

- No widely used standards
- A wild west
- Hard to scale federation if we can't scale provisioning
- Provisioning what? Identities, Credentials, Services
- De-provisioning? "We can do that later."
What to do about it

• Planned to start with product evaluations
• Got tangled up in terminology
• Take II: survey of current practices and needs
  • Identify trends
• A new product evaluation
  • Understand current product landscape
• Document best practices
Working group initiatives

• Best practices write-up
• Product comparison
• Catalog of SCIM schemas
• Bulk provisioning API definition
SCIM schema cataloging

• Goal: a catalog of known extensions to SCIM
• Progress: Created a Github repo with the core SCIM schema
  • Extensions???
  • It can't be that easy
  • Help us if you know of extensions
• Status: https://github.internet2.edu/tier/scim-schema
Bulk provisioning API

• Goal: Create API requirements for provisioning large batches
  • Pass requirements to TIER API WG to develop
• Progress: Created a list of use cases
  • Shared list with TIER API WG
• Status: a separate bulk API is not needed
  • Use cases to be used as tests for the API WG
  • Use cases: https://spaces.internet2.edu/x/koFyBw
Documenting best practices

• Completed survey analysis last fall
  • Reported at Technology Exchange
• Created high-level outline for write-up
• Preparing for product evaluations
Best practices outline

• Executive summary
• Problem statement
• Identity provisioning
  • Identity matching
  • Username assignment
  • Identifiers for services and target directories
  • Username changes
  • Social IDs
Best practices outline

• Identity lifecycle
  • State and affiliation changes
  • Deactivation or deletion

• Credential provisioning
  • Password rules and policies
  • Initial password setting
  • Assignment of additional authentication factors
  • Deprovisioning of credentials
Best practices outline

• Target directory provisioning
  • Linking identities between directories
  • Communicating updates to target directories

• Service provisioning
  • Provisioning models: when to provision
  • Reconciliation
  • State changes and fine-grained authorization
  • Deprovisioning and repatriation
Best practices outline

• Groups and roles
  • Types of groups
  • Guidance for architecting

• Auditing
  • Reporting
  • Attestation
  • Workflows to deprovisioning
Product evaluations

• Inspired by TIER Entity Registry WG
• Functional evaluation
• Open source and commercial
• Done by member schools and others
• Collaboration encouraged
What's it look like?

• Simple format
  • 3 questions for each section
  • Product maturity
  • How does the product do it?
  • What's missing?

• A few questions on
  • Licensing and support
  • API capabilities
  • Extensibility and customization
Next steps

• Completed product evaluations this summer
  • Evaluation started for Midpoint

• Produce product comparison

• Discover additional best practices

• Find needs and deficiencies
  • Share needs with TIER developers
Want to help?

• Anyone can help
• Join the working group
• Evaluate your favorite provisioning engine
• Contact Keith Wessel
  • kwessel@illinois.edu