Importance of User Deprovisioning from Services

Slávek Licehammer
slavek@ics.muni.cz

Masaryk University

International Symposium on Grids and Clouds 2016

Motivation

- Services require
  - Authentication
  - Authorization
  - Attributes of users
- Move from local registration to central services
  - Simplify user management for services
  - Users are managed outside the services
    - Identity federation (e.g. eduGAIN)
    - External IdM systems
  - Authorization is based on external information

Provisioning

- Method to deliver user information to services
  - Access rights
  - Authorization informations (groups, roles)
  - User attributes (name, e-mail, …)
- Commonly triggered by user sign in
- May create/update local user account
  - Local account is required by some services to keep user data

Provisioning

- Implementations
  - Just-in-time
    - SAML, X.509 certificates
  - Pull model
    - LDAP, SAML attribute authority, VOOT, SCIM, XML, ...
  - Push model
    - Needs endpoint for processing pushed data

Provisioning - service examples

- Access to wiki page or document server
- Grid job submission
- Collaboration tools (e.g. video conference)
  - Need to know users upfront
  - Have to use push model, or periodical pull

Deprovisioning

- Method to notify service about users who are no-longer authorized to use the service
- Necessary for services with persistent resources owned by users
  - Cloud infrastructures
  - Data storages
  - Reservation systems
- Notification is delivered without explicit user action (e.g. sign in)
- Reaction on notification depends on service

Deprovisioning

- Implementation
  - Periodical pull
  - Push model
- Transferred dataset
  - Changeset only
    - Need to assure consistency
  - Full state
    - May have performance issues
- Protocols
  - LDAP, VOOT, SCIM, JSON, XML, ...

Provisioning & deprovisioning

- Provisioning and deprovisioning are usually deployed together
- Provisioning all changes in user information
- Up-to-date user information on service level
  - Service is not dependant on IdM system
    - If authentication server is not part of IdM
- Include security incident mitigation
  - “Suspended” status of user is provisioned to service
  - Service will react appropriately

Identity and access management

- Distributed authorization management
  - Delegation of management rights
- Role for security team
  - Capability to suspend users
- Support for user life-cycle
  - Registration / import, expiration, renewal
  - Support also on service side
- Allow consolidation of user identity
  - Migrating user between institutions
  - Need to be supported on service level

Requirements for (de)provisioning

- Bare minimum
  - Support for user life-cycle
    - Create, delete users
  - Attribute / group management
- Additional requirements
  - Assigning access rights to use services
  - Detect changes within system
    - Decide which services are affected
  - Evidence of the services

Practical solution

- Existing IdM systems usually do not support deprovisioning
- Solution - external system connected to primary sources of user identity and attributes
- Perun - http://perun.cesnet.cz
  - Deployed on Masaryk University, Czech e-infrastructure, EGI FedCloud, ELIXIR
- Periodical synchronization data from primary sources or allow user self-registration
- Push new configuration to services

Summary

- Provisioning and deprovisioning notify services about changes in user attributes or state
- Deprovisioning is crucial for services with persistent user resources
- User life-cycle and attribute / group management is prerequisite
- Can be handled with external identity and access management system

Future challenges

- Standardized protocol for deprovisioning
  - SCIM notification
- Distributed identity and access management
  - Each IAM system manages part of access rights
    - Data forgery protection
  - Merge of user attributes

Thank you for attention

Slávek Licehammer
slavek@ics.muni.cz

Masaryk University

International Symposium on Grids and Clouds 2016