Could SCIM become lingua franca of Identity Provisioning

(Un)conference on Open Source Identity and Access Management, Vienna 18.02.2020

Peter Gietz, DAASI International
Agenda

- Why Standards in Open Source
- Short Introduction into SCIM
- Deployment examples
- SCIM lingua franca for identity provisioning
Why standards in Open Source

- OSS is not only about open source but also about interoperability and work division
  - No attempt to create golden cages
  - Rather it is important to interact with other products
- Reference implementations of standards are mostly if not always OSS
- In OSS clients and servers often are from different developers
- Open Culture with open standards vs. closed source and proprietary protocols
SCIM

- Originally “Simple Cloud Identity Management”
  - thus designed as provisioning standard for the cloud
- Then renamed to “System for Cross-domain Identity Management”
  - Thus a generalisation for any provisioning between different domains
  - “the open API for managing identities”
  - JSON and RESTful based lightweight approach to identity provisioning
- Version 1.0 (Dezember 2011), Version 1.1 (Juli 2012)
- Version 2.0 (September 2015)
  - Definitions, Overview, Concepts, and Requirements: RFC7642
  - Core schema: RFC7643
  - Protocol: RFC7644
Extensions not (yet?) RFCs

- **Soft delete of Users**
  - draft-ansari-scim-soft-delete-00, Expires: September 10, 2015

- **Hub change notification service**
  - Draft-hunt-scim-notify-00, Expires: September 9, 2015

- **Password and account status** extensions for managing passwords and password usage
  - Draft-hunt-scim-password-mgmt-00, Expires: September 30, 2015

- **Just-in-time provisioning** patterns in a protocol (such as SAML)
  - draft-wahl-scim-jit-profile-00.txt, Expires: August 2013

- **Mapping between SCIM and vCard**
  - Draft-greevenbosch-scim-vcard-mapping-03, Expires: August 16, 2014

- **Privileged Access Management**
  - Draft-grizzle-scim-pam-ext-01, Expires: April 21, 2018
SCIM Implementations

- http://www.simplecloud.info lists 45 implementations of SCIM 2.0 by
  - Apache Foundation, Atlassian, Beta Systems, Centrify, GitHub Inc, Gluu, Microsoft, Okta, Omada, One Identity, Oracle, Ping Identity, SailPoint, Salesforce, WSO2 Inc, and many others
  - 18 of these are open source
SCIM in a nutshell

- SCIM “is designed to manage user identity in cloud-based applications and services in a standardized way to enable interoperability, security, and scalability.” (RFC 7642)
- “SCIM's intent is to reduce the cost and complexity of user management operations by providing a common user schema, an extension model, and a service protocol” (RFC 7644)
- SCIM “provides a platform-neutral schema and extension model for representing users and groups and other resource types in JSON format. This schema is intended for exchange and use with cloud service providers.” (RFC 7643)
SCIM Schema

Resource

* id, externalId, meta

User

Group

EnterpriseUser

Others...
SCIM Schema

- Resource
  - ServiceProviderConfig
  - CoreResource
    - User
    - Group
  - Schema
    - EnterpriseUser

*id, meta
*externalId
Minimal representation of a user

```json
{
  "schemas": ["urn:scim:schemas:core:2.0:User"],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "userName": "bjensen@example.com",
  "meta": {
    "resourceType": "User",
    "created": "2010-01-23T04:56:22Z",
    "lastModified": "2011-05-13T04:42:34Z",
    "version": "W\"3694e05e9dff590\"",
    "location": "https://example.com/v2/Users/2819c223-7f76-453a-919d-413861904646"
  }
}
```
Only standardised extension enterprise user

{
    "schemas": [
    ],
    "id": "2819c223-7f76-453a-919d-413861904646",
    "externalId": "701984",
    "userName": "bjensen@example.com",
    "name": {
        "formatted": "Ms. Barbara J Jensen, III",
        "familyName": "Jensen",
        "givenName": "Barbara",
        "middleName": "Jane",
        "honorificPrefix": "Ms.",
        "honorificSuffix": "III"
    },
    ...
}
Only standardised extension enterprise user

employeeNumber
costCenter
organization
division
department
manager
Deployment examples

- midPoint → SCIM ICF Connector → Gluu
- midPoint → LDAP ICF Connector → LDAP
- midPoint → Gluu
- LDAP → Gluu
Deployment examples

midPoint API SCIM Overlay SCIM Client
Deployment examples
Why a lingua franca

- SCIM is supported by many vendors and developers
- SCIM has an extension mechanism
  - Different schema, same REST protocol
- In didmos2 we defined some internal extensions
  - Could be standardized
- SCIM can be used to integrate different open source products
- LDIF $\rightarrow$ DSML $\rightarrow$ SCIM JSON
Thanks!

Contact me at
peter.gietz@daasi.de