An Introduction to SCIM: System for Cross-Domain Identity Management

Nicholas Crown
UnboundID
Agenda

- Why Standards-Based Provisioning?
- History of Standards-Based Provisioning
- SCIM Overview
Why Standards-Based Provisioning?

- Need a standard way to create, read, update, and delete users (accounts) for both enterprise and consumer based digital identities
  - In the enterprise, password management and compliance were big drivers
- Interoperability is the hardest part
  - Different protocols and user schemas
- Provisioning connections are difficult to maintain and are fragile
  - Application revisions can require engineering effort
History of Standards-Based Provisioning

- 2000: eXtensible Resource Provisioning Management (XRPM) Access360 (now IBM)
- Active Digital Profile (ADPr) Business Layers (now CA)
- OASIS Provisioning Services Technical Committee begins work on SPML v1
- Information Technology Markup Language (ITML)-Account Provisioning Specification for Internet Business
- IBM proposes a competing standard WS-Provisioning; requirements fed into SPML v2 specification
- OASIS approves SPML v1
- OASIS approves SPML v2
- OASIS approves SPML v2
SPML Adoption

- Adoption by application developers was low
- Implemented in most of the provisioning systems, but not one system is SPML conformant
  - Application developers must build SPML-specific interfaces for each of the provisioning systems
  - Support was more a "checkbox" item
- Few applications support SPML
- Not supported by popular SaaS applications
- Since the 2006 approval of SPML v2, activity in the OASIS PSTC was non-existent
  - That is, until May of 2010
Genesis of SCIM

- Evolved from the Cloud Directory ("LDAP in the cloud")
  WG spawned at the 2010 Cloud Identity Summit
- Founding participants include some of the largest SaaS providers:
Genesis of SCIM

- Cloud Service Providers (SaaS, etc.) are all feeling the user provisioning pain:
  - “How do I provision a user account for service X?”
  - “How do I de-provision a user account from service X?”
  - “How do I update an existing account for service X?”
  - “How do I keep my organization’s users in sync with service X?”
  - “How do I manage groups?”

- How is it done today?
  - Manual (UI)
  - Bulk (CSV upload)
  - API
  - SAML Just-In-Time provisioning
SCIM

THE ENTERPRISE

YOUR IDENTITY

CLOUD PROVIDERS

- Single “pipe” to the cloud
- Standard REST API and schema
- Extensible
- CRUD
History of SCIM

- July '10: Conceived at Cloud Identity Summit
- May '11: Officially began at IIW 12
- Dec '11: Released 1.0 specification under OWF
- Mar '12: BoF at IETF 83
- Jun '12: IETF WG chartered
- Jul '12: 1st IETF WG meeting
- Aug '12: Released 1.1 specification under OWF
A Resource-Centric Model

- A resource is:
  - Attribute container
  - Name spaced
- An attribute is:
  - Simple or Complex
  - Single or Multi-valued
  - Typed
Schema

- Rich Information Model
- XML and JSON data models
- Concrete artifacts (User and Group)
- Usage language (MTI and recommended)
- Extensibility: Inheritance and mix-in
Example: User

```
{
  "schemas":["urn:scim:schemas:core:1.0"],
  "id":"2819c223-7f76-453a-919d-413861904646",
  "externalId":"bjensen",
  "meta":{
    "created":"2011-08-01T18:29:49.793Z",
    "lastModified":"2011-08-01T18:29:49.793Z",
    "location":"https://example.com/v1/Users/2819c223...",
    "version":"W/\"f250dd84f0671c3\"
  },
  "name":{
    "formatted":"Ms. Barbara J Jensen III",
    "familyName":"Jensen",
    "givenName":"Barbara"
  },
  "userName":"bjensen",
  "phoneNumbers":[
    {
      "value":"555-555-8377",
      "type":"work"
    }
  ],
  "emails":[
    {
      "value":"bjensen@example.com",
      "type":"work"
    }
  ]
}
```
Example: Ext User

```json
{
  "schemas": [
    "urn:scim:schemas:core:1.0",
    "urn:scim:schemas:extension:enterprise:1.0"
  ],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "bjensen",
  "userName": "bjensen",
  "urn:scim:schemas:extension:enterprise:1.0": {
    "employeeNumber": "701984",
    "costCenter": "4130",
    "organization": "Universal Studios",
    "division": "Theme Park",
    "department": "Tour Operations",
    "manager": {
      "managerId": "26118915-6090-4610-87e4-49d8ca9f808d",
      "displayName": "John Smith"
    }
  }
}
```
Example: Group

```
Type (User|Group)
{
    "schemas": ["urn:scim:schemas:core:1.0"],
    "id": "2819c223-7f76-453a-919d-413861904646",
    "displayName": "Tour Guides",
    "members": [
        {
            "value": "2819c223-7f76-453a-919d-413861904646",
            "displayName": "Babs Jensen",
            "type": "User"
        },
        {
            "value": "2819c223-7f76-453a-919d-413861904646",
            "displayName": "Mandy Pepperidge",
            "type": "User"
        }
    ]
}
```
Protocol

- Synchronous, HTTP, ReST
- CRUD + Search* + Discovery + Bulk*
- Simple MTI, Complex optional
- Extensible*, Versioned
- “cURL” friendly
Operations

- Create = POST https://example.com/{v}/{resource}
- Read = GET https://example.com/{v}/{resource}/{id}
- Update = PUT https://example.com/{v}/{resource}/{id}
- Delete = DELETE https://example.com/{v}/{resource}/{id}
- *Update = PATCH https://example.com/{v}/{resource}/{id}
- *Search = https://example.com/{v}/{resource}?filter={attribute} {op} {value} & sortBy={attributeName} & sortOrder={ascending|descending}
- *Bulk
Create Request

POST /Users HTTP/1.1
Host: example.com
Accept: application/json
Authorization: Bearer h480djs93hd8
{
  "schemas": ["urn:scim:schemas:core:1.0"],
  "userName": "bjensen",
  "externalId": "bjensen",
  "name": {
    "formatted": "Ms. Barbara J Jensen III",
    "familyName": "Jensen",
    "givenName": "Barbara"
  }
}
Create Response

HTTP/1.1 201 Created
Content-Type: application/json
Location: https://example.com/v1/Users/2819c223-7f76-453a-919d-413861904646
{
   "schemas": ["urn:scim:schemas:core:1.0"],
   "id": "2819c223-7f76-453a-919d-413861904646",
   "externalId": "bjensen",
   "meta": {
      "created": "2011-08-01T21:32:44.882Z",
      "lastModified": "2011-08-01T21:32:44.882Z",
      "location": "https://example.com/v1/Users/2819c223-7f76-453a-919d-413861904646",
      "version": "W:\"e180ee84f0671b1\"
   },
   "name": {
      "formatted": "Ms. Barbara J Jensen III",
      "familyName": "Jensen",
      "givenName": "Barbara"
   },
   "userName": "bjensen"
}
Security: Protocol

- Service provider
  - Server-side SSL to authenticate to the consumer
  - Also sets up session encryption

- Consumer
  - Basic authentication (username and password) – OK for testing
  - OAuth – higher identity assurance, at the expense of additional complexity
  - X.509 (mutually-authenticated SSL) – provides higher assurance, at the expense of additional complexity
    - When tied to hardware, X.509 provides the highest identity assurance
Security: User

```
{
  "id": "2819c223-7f76-453a-919d-413861904646",
  "externalId": "bjensen",
  "name": {
    "formatted": "Ms. Barbara J Jensen III",
    "familyName": "Jensen",
    "givenName": "Barbara"
  },
  "password": "maybe_plaintext",
  "roles": [
    {
      "value": "RA"
    }
  ],
  "groups": [
    {
      "value": "Student"
    }
  ],
  "entitlements": [
    {
      "value": "delete users",
      ...
    }
  ]
}
```
Within Scope

- CRUD operations for
  - Users
  - Groups
  - Possibly other identity related objects (e.g. Devices)
- Bulk operations
- Protocol Binding for SAML, LDAP
- Extension semantics (schema & protocol)
Out of Scope

- Defining new authentication/authorization frameworks or mechanisms
- Defining access control mechanism or semantics
- Managing non-identity related resources
Current SCIM Topics

- Targeting
  - Enables the same SCIM service to provision to multiple repositories
  - Similar to the SPML provisioning service point and provisioning target
  - Introduces additional complexity, particularly if the targets wish to share resource attributes

- externalid
  - Make it optional
    - Some customers may be looking at the service provider's ID attribute as the permanent user identifier
Applying SCIM - What it Means for You

- Check out the draft specification on the IETF website and the open source implementations that are available today
  - http://datatracker.ietf.org/wg/scim/
- Evaluate how you are currently provisioning to cloud-based services
- Determine your current provisioning vendor’s plan for supporting SCIM – if any