SCIM Schema

IETF 86 – March 15, 2013

Kelly Grizzle

kelly.grizzle@sailpoint.com

Overview

- Schema shortcomings around extensibility were discovered during vCard discussion
- Lack of formal “references” – issue #33
- Issues with extension mechanism – issue #38
- Process for registering extensions – issue #30

Extensibility – Group Example

- Group membership is modeled in SCIM through the Group “members” attribute and the User “groups” attribute.
- Q: What happens if you want to store more information about a user’s group assignment? For example, expiration date.
- A: This can be modeled as a new resource type. ***However, SCIM data types don’t handle references well.***

Extensibility – References

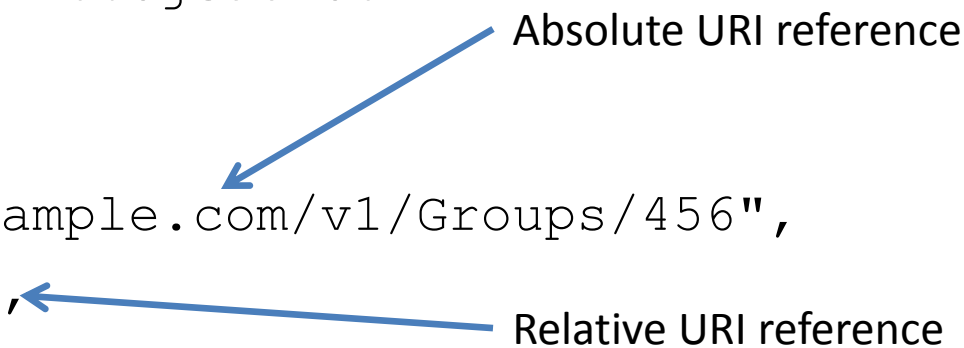
- Issue #33 opened to add “reference” data type, which is a reference to another SCIM resource.
- User, Group, EnterpriseUser schemas changed to use reference where appropriate.
- Schema resource can include “referenceTypes” for attributes to specify which SCIM object types can be referenced for a given attribute.
- See proposed changes in issue #33.

http://trac.tools.ietf.org/wg/scim/trac/ticket/33

Extensibility – Group Example

```
GET /GroupMemberships/123 HTTP/1.1
Host: example.com
Authorization: Bearer h480djs93hd8

{
  "group": "https://example.com/v1/Groups/456",
  "user": "/Users/789",
  "assigned": "2013-03-01T04:56:22Z",
  "expiration": "2013-03-31T04:56:22Z"
}
```



More Extensibility Problems – Issue 38

- Current schema document is light on details around extensibility.
- It is impossible to tell which extensions a resource contains. The “schemas” attribute may not be enough.
- Possibility for collisions between attribute names within a schema (if it contains multiple extensions).
- Need more detail about how extensions are defined.
  - Can you add new sub-attributes to a complex attribute?
  - Can’t easily share extensions between multiple resource types.

More Extensibility Problems – Issue 38

- Proposed solution
  - Clearer definitions of schema vs. resource vs. extension.
  - Separate ResourceTypes and Schemas resources
    - Resource type has a URL and information about resource.
    - Schema has attributes used by a resource type. Schemas can be used as primary attributes or extensions for ResourceTypes.
  - Resources reference resource types instead of schemas

http://trac.tools.ietf.org/wg/scim/trac/ticket/38

ResourceTypes Resource

```
GET /ResourceTypes
[
  {
    "name": "User",
    "endpoint": "/Users",
    "schema": "urn:scim:core:User:1.0",
    "extensions": [
      "urn:scim:schemas:extension:enterprise:EnterpriseUser:1.0",
      "urn:edu:Staff:2.0"
    ]
  },
  {
    "name": "Group",
    "schema":"urn:scim:core:Group:1.0",
    "endpoint":"/Groups"
   }
]
```

Schemas Resource

```
GET /Schemas
[
  {
    "id": "urn:scim:core:User:1.0",
    "name": "User",
    "description": "This is a basic User",
    "attributes": [
      {
        "name": "id",
        "type": "string",
        "multiValued": false,
        "description": "Unique identifier....",
        "readOnly": true,
        "required": true,
        "caseExact": false
      },
      ...
    ]
  },
  ...
]
```

Example User using resourceType

```
GET /Users/123

{
  "username": "bjensen",
  "meta": {
    "resourceType": "User",
    ...
  }
  ...
  "urn:scim:schemas:extension:enterprise:EnterpriseUser:1.0": {
    "employeeId": "12345"
  }
}
```

Note: Lack of “schemas” attribute. Schemas are determined by looking at referenced ResourceType.

Extension Registration – Issue 30

- vCard has a process around registering extensions with IANA.
  - http://tools.ietf.org/html/rfc6350#section-10.2
- SCIM could benefit by adopting a similar process.
  - Could help us in defining what an extension is and how to use it (issue 38).
  - Creates a registry of extensions.
- Volunteers?

http://trac.tools.ietf.org/wg/scim/trac/ticket/30