SCIM Intro

Janelle Allen and Danny Zollner

November 11th, 2021 – IETF 112 / Virtual

What is SCIM?

“System for Cross-domain Identity Management”

- Protocol designed for sharing data across identity contexts
- Consists of the communication protocol and the core schema
  - Allows for extensibility

“builds upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration” rfc7643

“In essence, make it fast, cheap, and easy to move users in to, out of, and around the cloud.” rfc7642

Why SCIM?

- Abstracts away underlying data structure
- Treats every site/domain/whatever the same, enables scale


```
{
  "schemas":
   ["urn:ietf:params:scim:schemas:core:2.0:User",
     "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"],
   "id": "34234d23-7f76-453a-56765765765",
   "userName": "jsmith@example.org",
   "name": {
   "formatted": "Ms. Jane Smith",
   "familyName": "Smith",
   "givenName": "Jane"
    },
    "phoneNumbers": [
    {
       "value": "432-123-4566",
      "type": "home"
    }],

    "emails": [
    {
  "value": "jsmith@example.org",
  "type": "work",
  "primary": true
   }]
}
```


```
dn: dc=myapp,dc=com
objectClass: inetOrgPerson
sn: "Smith"
givenName: "Jane"
homePhone: "432-123-4566"
mail: jsmith@example.org
```

The SCIM Protocol RFC 7644

- Simple RESTful APIs designed for developer ease of use
  - uses HTTP methods (*verbs*) GET, POST, PUT, PATCH, DELETE for creating and modifying the data via SCIM standard JSON payloads to the resource endpoints (*nouns*)
- Standardizes methods for clients to communicate with servers (*Service Providers*)
- Provides a client the ability to discover resources and server config via three discovery endpoints

Service Provider: An HTTP server (rfc2616) which exposes the standard SCIM APIs for Create, Read, Update & Delete operations for a SCIM Client

Available Standard SCIM Endpoints

Discovery	Endpoint	Description	Supported REST Verbs
	/Users	Create, Read, Update, Delete on user data	GET, POST, PUT, PATCH, DELETE
	/Groups	Create, Read, Update, Delete on group data (*including membership)*	GET, POST, PUT, PATCH, DELETE
	/Me	Create, Read, Update, Delete on users own data	GET, POST, PUT, PATCH, DELETE
✔	/Schemas	Retrieve available schemas	GET
✔	/ResourceTypes	Retrieve available resource types	GET
✔	/ServiceProviderConfig	Retrieve available config on the server (ServiceProvider)	GET
	[prefix]/.search	Read and returns queried data	POST
	/Bulk	Contains series of operations to the server in bulk	POST

Examples of REST operations

REST Operation	Resource	Result
POST	/Users	Creates new resource
GET	/Users	Returns all resources
GET	/Users?filter=userName eq “user@domain.com”	Returns all resources matching filter
GET	/Users/123	Returns resource with matching id value
PUT	/Users/123	Updates all attributes on resource
PATCH	/Users/123	Updates only specified attributes on resource
PATCH	/Users?filter=userType eq “Intern”	Updates all resources matching filter
DELETE	/Users/123	Deletes resource with matching id value

The SCIM Core Schema RFC 7643

- Defines a minimal common set of attributes representing user and group data along with an enterprise extension for user data
- Provides a method for organizations to extend SCIM
  - Schemas
  - Resource types
- Custom schemas may be permanently registered with IANA https://www.iana.org/assignments/scim/scim.xml

Example SCIM User: GET /Users/123

name: single-valued complex attribute

The components of the user's name

phoneNumbers: multi-valued complex attribute with type for meaningful value to human user

emails: multi-valued complex attribute

Canonicalized value with type to provide meaningful value to human user

Resource Schema Representation:

https://datatracker.ietf.org/doc/html/rfc7643#section-8.7.1

{

"schemas": ["urn:ietf:params:scim:schemas:core:2.0:User", "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"],

"id": “123",

"**name**": { "formatted": "Ms. Jane Smith", "familyName": "Smith", "givenName": "Jane" },

"**phoneNumbers**": [{ "value": "432-123-4566", "type": "home" }],

"**emails**": [{ "value": "jsmith@example.org", "type": "work", "primary": true }]

"userName":"jsmith@example.org",

"meta":{...}

}

Attribute Data Types

- String
- Boolean
- Decimal
- Integer
- DateTime
- Binary
- Reference (a URI to a resource)
- Complex (a composition of simple attributes)

And we all lived happily ever after, until...

- Usability
  - Spec ambiguity led to multiple ways to implement causing interoperability challenges and data corruption
  - Limited guidance on groups, roles, entitlements
  - Common attributes not fully defined in 7643

- Improvements
  - Bulk operations are not asynchronous
  - Pagination limitations
  - Core Schema Extensibility

- New and Emerging
  - Limited privileged access management (in draft)

Other… Papercuts

Goals of SCIM NextGen

- Improve the overall best practices and guidance
  - Profiling SCIM relationship with other Identity Protocols
- Account State and Soft Deletion
- Reduce areas of ambiguity and provide more prescriptive examples
- Schema enhancements for HR, Enterprise Group, privileged access management
- Advanced automation scenarios
- Enhanced data handling for larger data sets

https://datatracker.ietf.org/doc/charter-ietf-scim/