IETF 114: SCIM Schemas and Protocol Topics

Agenda: Schema and Protocol

Has a draft(current or expired):

- Cursor-based pagination - draft-peterson-scim-cursor-pagination-00 (ietf.org)
- Multi-valued attribute pagination & filtering - draft-hunt-scim-mv-filtering-00 (ietf.org)
- Soft deletion – draft-ansari-scim-soft-delete-00 (ietf.org)
- Roles and entitlements draft – draft-zollner-scim-roles-entitlements-extension-00 (ietf.org)

No current or expired draft:

- Change detection/delta query
- Expansion on account status
- HR Schema
- Resource URL Security
- Modern Security BCP

Topics with existing drafts

Protocol: Cursor-based pagination

Draft Location

https://datatracker.ietf.org/doc/html/draft-peterson-scim-cursor-pagination-00

New query parameters and response attributes

- Cursor
- Count
- nextCursor
- previousCursor

Use cases

- Efficient traversal of large sets of results

Example Request:

```
GET /Users?count=10
Host: example.com
Accept: application/scim+json
Authorization: Bearer U8YJcYYRMjbGeepD
```

Example Response:

```
{
"totalResults":100,
"nextCursor":"VZUTiyhEQJ94IR",
"schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
"Resources":[{ ... <ten results> ... }
]
}
```

Protocol: Multi-valued attribute pagination & filtering

Draft Location

https://www.ietf.org/archive/id/draft-hunt-scim-mv-filtering-00.txt

Expanded use of paging & filtering parameters

- Paging and filters appended to attributes

Use cases

- Efficient traversal of large sets of values for multi-valued attributes
- Efficient filtered retrieval of select values on a multi-value attribute

Example Request:

```
GET /v2/Groups?filter=displayName sw 'Group'& \ attributes=*,
        members[type eq \"Group\"&count=5&startIndex=1]
Host: example.com
Accept: application/scim+json
Authorization: Bearer h480djs93hd8
```

Example Response

```
{
   "schemas": ["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
   "totalResults": 2,
   "Resources": [
    {
      "id": "c3a26dd3-27a0-4dec-a2ac-ce211e105f97",
      "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
      "displayName": "Group A",
      "meta": {...
        "members.cnt":1
      },
      "members": [
       {$member1}
       ] },
    {
      "id": "6c5bb468-14b2-4183-baf2-06d523e03bd3",
      "schemas": ["urn:ietf:params:scim:schemas:core:2.0:Group"],
      "displayName": "Group B",
      "meta": {...
        "members.cnt":7
      },
      "members": [
        <five members>
      ]
    }
   ]
}
```

Protocol: Soft Deletion

Draft Location

https://datatracker.ietf.org/doc/html/draft-ansari-scim-soft-delete-00

New query parameters and response attributes

- isSoftDeleted (bool)

Use case

- Protection for data and resource reference links being lost via holding resources in a “soft deletion” state after a SCIM DELETE request. From this state resources can then be restored(undelete) or hard deleted.

Example Request:

GET /Users/37e5c68b-9c08-443b-a38d-3c5299abe9ee

Example Response:

404/Not Found

Example Request:

GET /Users/37e5c68b-9c08-443b-a38d-3c5299abe9ee?isSoftDeleted=true

Example Response:

200/OK

{
"schemas": ["urn:ietf:params:scim:schemas:core:2.0:User"],
"id": "37e5c68b-9c08-443b-a38d-3c5299abe9ee",
“softDeleted”:true,
…
}

Protocol: Soft Deletion – Proposed Additions

2.1: Schema Extension - additional attributes

hardDeletedAfter - DateTime - displays date that resource will be permanently deleted (purged out of soft-deletion store)

2.2: ServiceProviderConfig - additional attributes:

daysHardDeletedAfter - Integer - states how many days objects will remain in soft deletion state

Alternative approach: Make complex with sub-attributes for the following:

1. Resource type
2. Does this object ever hard delete automatically
3. If #2 is true, how long does object remain in soft delete state
4. How long after hard deletion (if ever) do unique identifiers (userName, possibly emails) recycle and become available?

“softDeletionConfig”:[{
"resourceType":“User",
"hardDeletesAutomatically":true,
"daysHardDeletedAfter":30
“identifierRecycleInfo”:{
“uniqueIdentifiersRecycle”:true,
“daysRecyclesAfter”:365
}

}]

Schema: Roles and Entitlements

Draft Location

https://datatracker.ietf.org/doc/html/draft-peterson-scim-cursor-pagination-00

New resource types

- /Roles
- /Entitlements

Use cases

- Represent accepted values for user resource's "roles" and "entitlements" attributes in new resource types so that clients can use role and entitlement information to make successful SCIM requests and assist with management and assignment of values to users

Example Request:

```
GET /Roles
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

Example Response:

```
{ "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],

…,
"Resources":[
{
        "value":"user“,
        "display":"User“,
        "enabled":True

},
{
        "value":"teamlead“,
        "display":"Team Leader“,
        "enabled":True
} ] }
```

Topics without drafts

Protocol: Change Detection/Delta Query

No Draft Written

Use cases

- Tool for improving scale/efficiency for pull-based scenarios – common example being human resources data hosted by a SCIM service provider being retrieved by a SCIM client on regular intervals. A parameter to request only resources that have changed since the last time a similar query was made allows for only retrieving relevant resources.

Example

GET /Users?deltaToken=3a1d77dc-12b6-44ce-ace9-b3df2e844d1d

Schema: Human Resources Schema

No Draft Written

Use case

- Human Resources/Human Capital Management providers house data that is frequently used in provisioning/IAM processes. HR/HCM data does not align with the SCIM 2.0 core user schema very well. Creation of a generic HR/HCM schema will help to standardize attribute naming conventions for HR/HCM data in SCIM, improving interoperability.

Schema: Account Status Context

No Draft Written

Use cases

- The “active” attribute on the user resource provides limited context. Proposal is to add a new attribute such as “accountStatus” to the user resource schema and include additional information on the state of the user.

Protocol: Securing reference URL access

No Draft Written

Use cases

- Reference attributes such as photos require a URL to a resource to be provided. The SCIM 2.0 standard currently does not provide any security guidance for how to handle authorization for these URLs, which has been a blocker for some for adoption of the photos attribute. Exposing open anonymously accessible image files over the internet is not acceptable, and without a standard to address authorization there are considerable interoperability challenges that limit usage today.

BCP: Modern Security Profile

No Draft Written

Use cases

- Since the introduction of SCIM 2.0 some of the features mentioned in the standard have fallen out of industry best practices. A draft detailing modern guidance on best current practices on security may be needed.

Example suggestions

- Drop support for basic auth when authorizing to SCIM service providers
- Do not use “password” attribute for user resources in most scenarios (allowance for legacy systems)