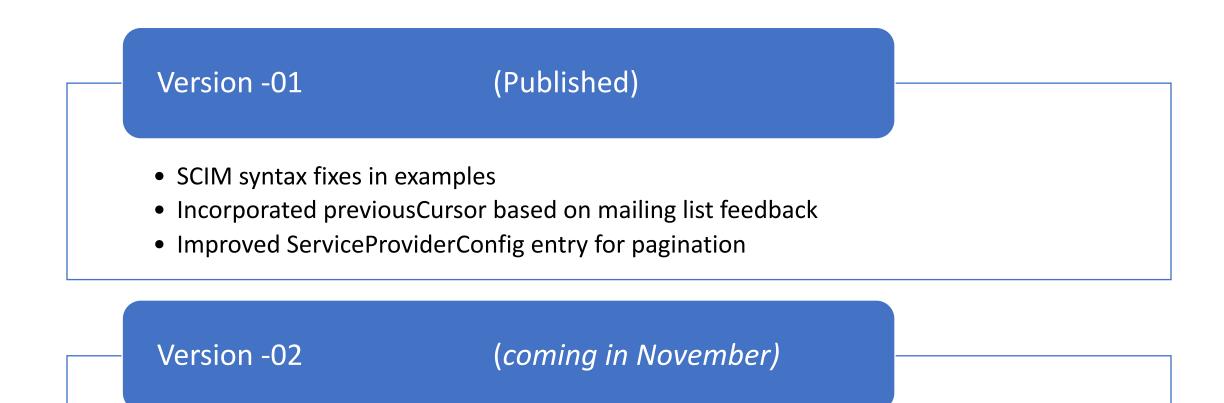
Cursor-based pagination updates



• Let us know if you have any additional feedback on the draft

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

Pagination, SCIM Events and (future) delta query drafts

Previous concerns expressed about the coexistence of these drafts due to concerns on overlapping scope

Matt and Danny do not see the concern – summary of the use cases behind each below

Pagination

- Efficient retrieval of results either subset(query) or all
- Needed for clients to get initial set of data and to refresh after data issues, configuration changes, etc.

SCIM Events

- Notification of high-priority changes account state, password changes, etc
- Can trigger SCIM client to pull/refresh resource
- Not universally implementable inbound connectivity requirements, additional SSE infrastructure requirements, and increased complexity of implementation/cross-service integration are all a concern

Delta Query

- Needed for synchronization use cases to improve efficiency of maintaining accurate state on large sets of resources
- Not solved by SCIM events due to above challenges + implementer variance in whether events can be retrieved in the event of loss by the event receiver
- A watermark-based delta query would be more easily implemented and more easily built to be repeatable, allowing requery in the event it was required

Referential Value Location Draft

What it is

Extension to urn:ietf:params:scim:schemas:core:2.0:Schema that adds new properties to schema definition

What it does

- Extended properties allow the schema properties of an attribute to convey "This attribute only accepts a limited set of values, and those values are searchable on XYZ attribute on XYZ resource"
- i.e.: "The User manager.value sub-attribute only accepts values of the User resource's 'id' attribute"

Larger opportunity

- Are there other new schema properties that are needed? i.e.: Cardinality
- Should this draft change to a broader new/advanced schema properties extension?

https://datatracker.ietf.org/doc/draft-zollner-scim-referential-value-location/

Roles and Entitlements

What is it?

• Adds new /Roles and /Entitlements endpoints and schema for client discovery of available values for User resource's roles and entitlements attributes

Status

Currently in call for adoption – please comment on mailing list

Other opportunities

- Expanding role/entitlement manipulation to have "members" attribute to improve scalability when many users needs to have the same role added
- Guidance on how to use type sub-attribute with roles/entitlements
- Roles/entitlements that are prerequisites or cannot be combined with

https://datatracker.ietf.org/doc/draft-zollner-scim-roles-entitlements-extension/

Upcoming Work

HR Schema

- Generalized HR "Worker/Employee" schema (separate from User) to standardize how HR providers represent their data
- Improves ease of interoperability/integration between SCIM clients that need to consume data from many HR providers

Delta Query

• Change detection is needed for pull-based scenarios where a client is regularly checking the state of a large set of results

Security BCP

- Provide modern guidance on security best practices when implementing SCIM
- Strong advisement against user/pass authentication, use of password attribute in non-legacy scenarios, etc.

Reference Attribute URL Authorization

- Address the problem of how to standardize securing URLs for attributes like 'photos' where the value is an HTTP URL pointing to a likely internet-accessible resource.
- Provisioning of photos is not widely adopted in internet-facing SCIM implementations in part because of the security concerns