SCIM Schemas and Protocols Work

IETF 113 – Vienna
Danny Zollner & Janelle Allen
Wednesday, March 23rd, 2022
Current Charter

• Charter: [https://datatracker.ietf.org/wg/scim/about/](https://datatracker.ietf.org/wg/scim/about/)

• Progressing SCIM 2.0 from Proposed standard -> Internet standard
  • Is there significant value here?
  • What level of error correction, clarity enhancement is permissible without issuing a new version and RFC series?

• Charter proposes a lot of schema and protocol enhancements
  • Types of changes proposed in charter require new RFCs
    • SCIM vNext- 2.1 or 3.0?
    • Or do we progress 2.0 to Internet Standard and extend with extension RFCs?
Work proposed in charter

Revision of RFC7643 and RFC7644 that will include:

• Profiling SCIM relationships with other identity-centric protocols such as OAuth 2.0, OpenID Connect, Shared Signals, and Fastfed
• Updates to the evolution of the externalid usage
• Updates to account state for capturing context of the state or change in state of the users account
• Multi-Value Query Filtering and Paging (will use draft-hunt-scim-mv-paging as input)
• Define a method for coordinating resources between domains:
  • Incremental approach to synchronization
  • Consider building off of RFC8417 and draft-hunt-idevent-scim
• Support for deletion-related goals including:
  • Handling Deletes in SCIM Servers that don’t allow Deletes (Soft Deletes) (will use draft-ansari-scim-soft-delete as input)
• Support for advanced automation scenarios such as:
  • Discovery and negotiation of client credentials
  • Attribute mapping
  • Per-attribute schema negotiation
• Enhance the existing schema to support exchanging of human resources, enterprise group and privileged access management (will use draft-grizzle-scim-pam-ext as input)
IETF SCIM WG GitHub

- New repos created for schema and protocol/API work

- Errata, ambiguity clarification to be proposed via GitHub issues
  - Enables per-issue discussion on possible solutions

- Work on 2.0 Proposed -> Internet Standard should be separated in GitHub from work on SCIM vNext

- 2.0 edits directly in XML, vNext drafting/editing in Markdown/Kramdown
Papercuts for schemas and protocol

• Survey on implementation of concepts proposed for being cut
  • Have concepts been successfully implemented in a way that allows cross-platform interoperability to occur?
  • Are some concepts outdated, insecure, not in alignment with use cases?
    • Basic auth
    • Passwords
    • Photos
    • (Open to other nominations for concepts to consider cutting)
XY Problem

• Are some concepts useful but potentially outside of the scope of what the SCIM standard aims to address?
  • Some decisions on cuts and edits to 2.0 should wait until after use cases are revised

• Is work to revise use cases targeted at 2.0, vNext(2.1/3.0/etc) or both?
Recap

• How big of changes can we make while remaining SCIM 2.0?
• Bigger changes – new version or a (long) series of extensions?
• Do we push back schema/protocol milestones to wait for use cases?