What is SCIM? Phillip Hunt and Nick Wooler

SCIM characteristics (started note-taking in the middle)

- HTTP
- Robust
  - going cross-domain, not every attribute interest to all domains
  - free to ignore an attribute
  - leads to flexibility

SCIM 3.0?

- SCIM structure
  - resource: users and groups
  - how to extend the users to enterprise
  - schema as a generic document handler
  - schema extension allows for local customizations
  - extensions to IoT/password managers
- Who is using it
  - 65k+ simple-cloud.info - not all registered

Body of Work P.Lanzi, Matt Peterson

- What we want to address
Body of Work - Matt Peterson and Paul Lanzi

- What we, as a community, want to address:

  Schemas:
  - A better process to define schemas, using these schemas as test cases: Exchanging HR information, exchanging Enterprise group information, Privileged Access Management

  Pagination:
  - draft-hunt-scim-mv-paging-00
  - draft-peterson-scim-cursor-pagination-00

  Synchronization-related functionality:
  - Initial 'download' of synced objects and ongoing sync

  Best practices for use of externalId:
  - How are implementation using externalId? What's the best practice?

  Privileged Access Management:
  - Expanded PAM use cases based on draft-grizzle-scim-pam-ext-01

  Question:
  - Is there anything we've missed?

- want to take to publication, since mature specifications

- Collaboration tool for input/feedback
  - [https://padlet.com/paulpad1/ietf111_sins](https://padlet.com/paulpad1/ietf111_sins)
  - Answer by commenting on the questions
  - vote by Liking the improvements you think are important
    - categorized following the conversation in the ML
  - Pagination: handling large datasets
    - all members of the group
  - synchronization-related functionality
    - SCIM client wants to keep local copy of the information they retain
    - popular for IDM systems/application that need to enforce authz based on the objects they retrieve using SCIM
    - another use-cases: entire users are deleted/group memberships are removed
  - RFC7643: externalId
    - want to head more scenarios - can be confusing how to use it
    - do we need externalId?
  - PAM (priviledged access management)
    - use SCIM to grant access
- SCIM not good enough for this?
  o some other interest

- How the likes/comments looked like at the point of presentation

- Comments
  o SCIM might help with IoT
  o why is SCIM restricted to users/roles? Can’t we publish entitlements?
    ▪ other entitlements provisioned in the same way
    ▪ any role assignment within cloud provider that grants access to the users/groups needs to be done through API - no SCIM
  o Inconsistencies
    ▪ missing best practices/profiling
  o people free to define whatever schema - can IANA register if wish
  o SCIM defined roles
  o how to extent to add metadata such as expiry dates
    ▪ now will define an enterprise group that will carry all metadata
    ▪ ppl just add the object and off you go
  o interop tests if schemas are better refined - scaling
  o security piece - HR schema
• advantage to make requirements around

Proposed Charter - Pam DIngle

Desired Outcomes

A re-chartered SCIM WG can accomplish:

• Easier Understanding (therefore more adoption)
  ○ Better address of common implementation roles & patterns
  ○ Clarification of terms
• Reduction of Known Pain Points
  ○ Almost a decade of implementation experience brought to bear
• Optimization for Multi-Cloud Scenarios
  ○ Examination of multi-tenant representations
  ○ Examination of how SCIM fits into greater cloud platform architectures
• Compatibility with modern security best practice

• can help adoption in the changed world
• papercuts of the small things that prevent easierconnection

How could this charter unfold (priority list)

• CAVEAT: this is a non-WG forming BoF, but if enough interest can proceed to WG formation - please comment

1. change the language to be more modern
   ○ ex) few cloud providers to be talking to each other, new use-cases, etc.
   ○ clarify - ex) SCIM client that pushes/pulles, etc.
2. any changes in core language
   ○ ex) security review - how to get an OAuth key
   ○ need implementor’s pain feedback
3. schema workshopping
   ○ specialized participation
4. extension breakouts
   ○ to prevent fragmentation of the conversation
5. interop testing
Next steps

- Need to be careful with starting schema standardization
  - implementations do a lot of private schemas
  - might get us stuck in details as each company has separate definitions
  - a world where you can use your own schema in a standardized way on top of the schemas built into the vendor products: ex - EDU space
- Moving SCIM spec into standard vs extensions and changes - seems conflicting
  - for example, compatibility with SCIM 1.0?
- how much do we want to work on synchronization?
  - how tight do you want synchronization to be?
  - we might not be ready to work on solid concept yet, need a strong use-case document that describes the requirements?
  - for example, paging described as a solution to synchronization - dumbing data so becomes expensive when you pay for bytes
    - potentially - basing off identity/security events -> going to event notification rather than synchronization
    - proposal to add to charter “work on notification mechanism in SCIM that can be used for synchronization”
  - worth building consensus on agreeing on the problem first
  - collection of SCIM services in imp, but want to avoid being pulled by spectrum of protocols from LDAP days
- Enough authors :)
- Anyone opposed to a WG chartered along this charter?
  - no one
- No IAB questions

How to proceed

1. Clarify what body of work is needed
2. how we prioritize it

- Slightly refine the charter, prioritize and proceed to the WG
  - have a WG with the same name?
discussion continues at scim@ietf.org

- https://www.ietf.org/mailman/listinfo/scim