SCIM Industry Next Steps (SINS)

IETF 111 BoF Meeting

29 July 2021

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Agenda

What is SCIM? | N. Wooler, P. Hunt

Body of Work | P. Lanzi, M. Peterson

Proposed Charter Review | P. Dingle

Next Steps | BoF Chairs

Logistics

Chairs

- Barry Leiba
- Nancy Cam Winget
- Morteza Ansari (honorary)

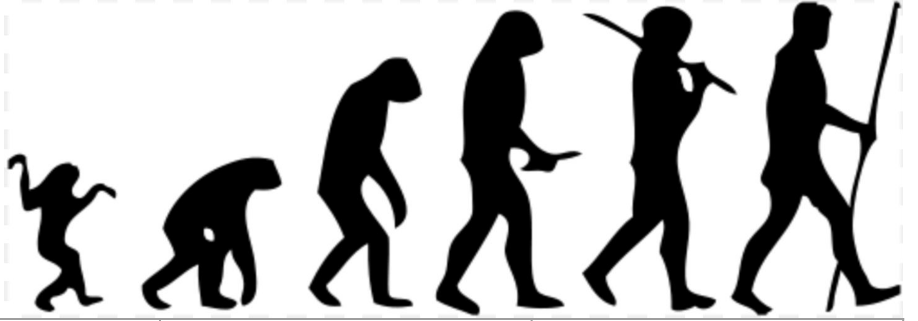
Community

https://github.com/SCIM-Interest-Group/

SCIM Mailing List (ietf.org)

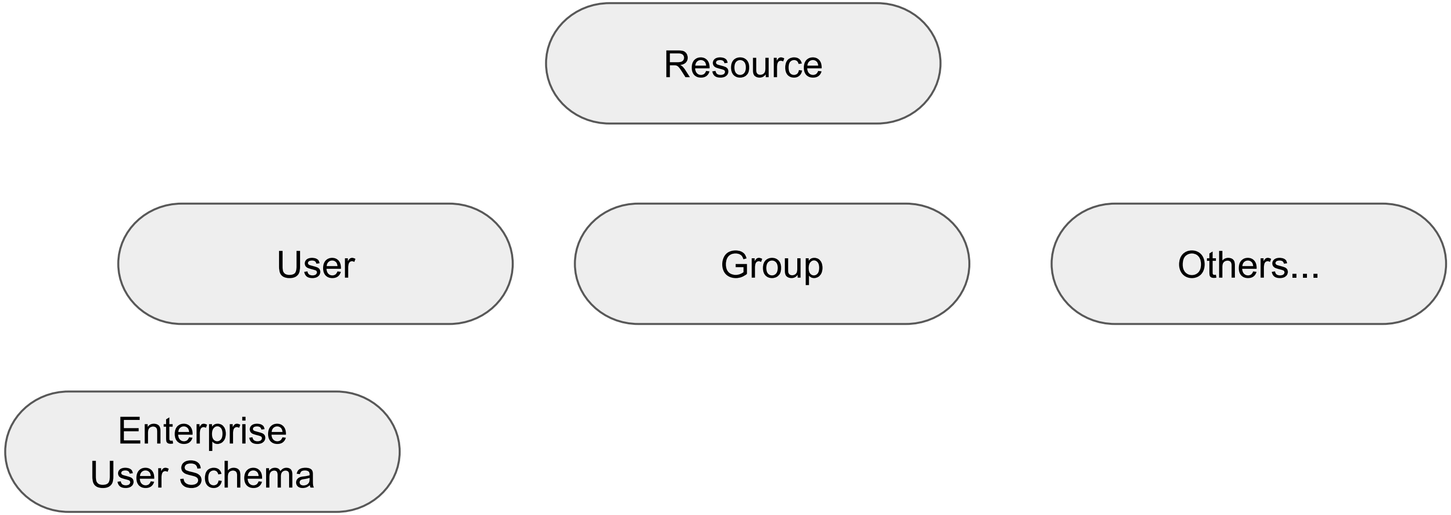
What is SCIM?

Evolution of SCIM



	Before SCIM	SCIM 1.0	SCIM 2.0	SCIM 3.0
Business Problem	Identity Silos within the enterprise	Bridge identity to the cloud	Identity at cloud scale	Identity & security at cloud scale?
Standard or Charter Objective	DSML SPML Federated / Virtual Directories RESTful APIs	SCIM 1.0 /Discovery /User /Group Restful Identity JSON VCard(ish)	SCIM 2.0 Identifier stability /Bulk Ops PATCH, HEAD Filters (valuePath) Extensibility Robust* rules	?
What was missing?	Consensus on Protocol, API, Format (ASN1, XML, JSON), Complex Attributes	Multi-value operations	UI paging Multi-cloud co-ord Sub-attr extens	

What is it?



Resource

User

Group

Others...

Enterprise
User Schema

Who is using it?

http://www.simplecloud.info/#Implementations2

65+

Implementations

100K

Enterprises

500M

Users

100B

API CAlls

Body of Work

Body of Work - Matt Peterson and Paul Lanzi

- How we will address the challenges stated in the Introduction
  - We will introduce new schemas, transports, etc. to solve:
    - New and emerging use cases
    - Papercuts with existing use cases
  - We will drive proposed standards forward to Internet Standards
    - RFC 7643 (SCIM Core Schema), 7644 (SCIM Core Protocol)
    - Justification: Level of maturity and adoption
    - *[look to pam's email discussion with mark wahl for more info re: justification for doing this as part of our work]*

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:

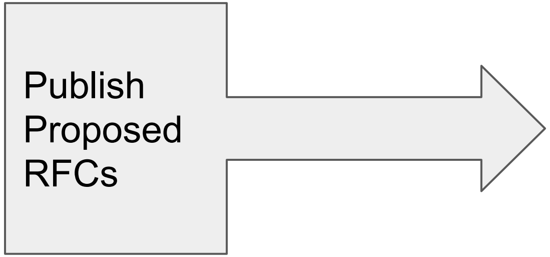
- How are implementation using externalid? What’s the best practice?

Privileged Access Management:

- Expanded PAM use cases based on draft-grizzle-scim-pam-ext-01

Question:

- Is there anything we’ve missed?

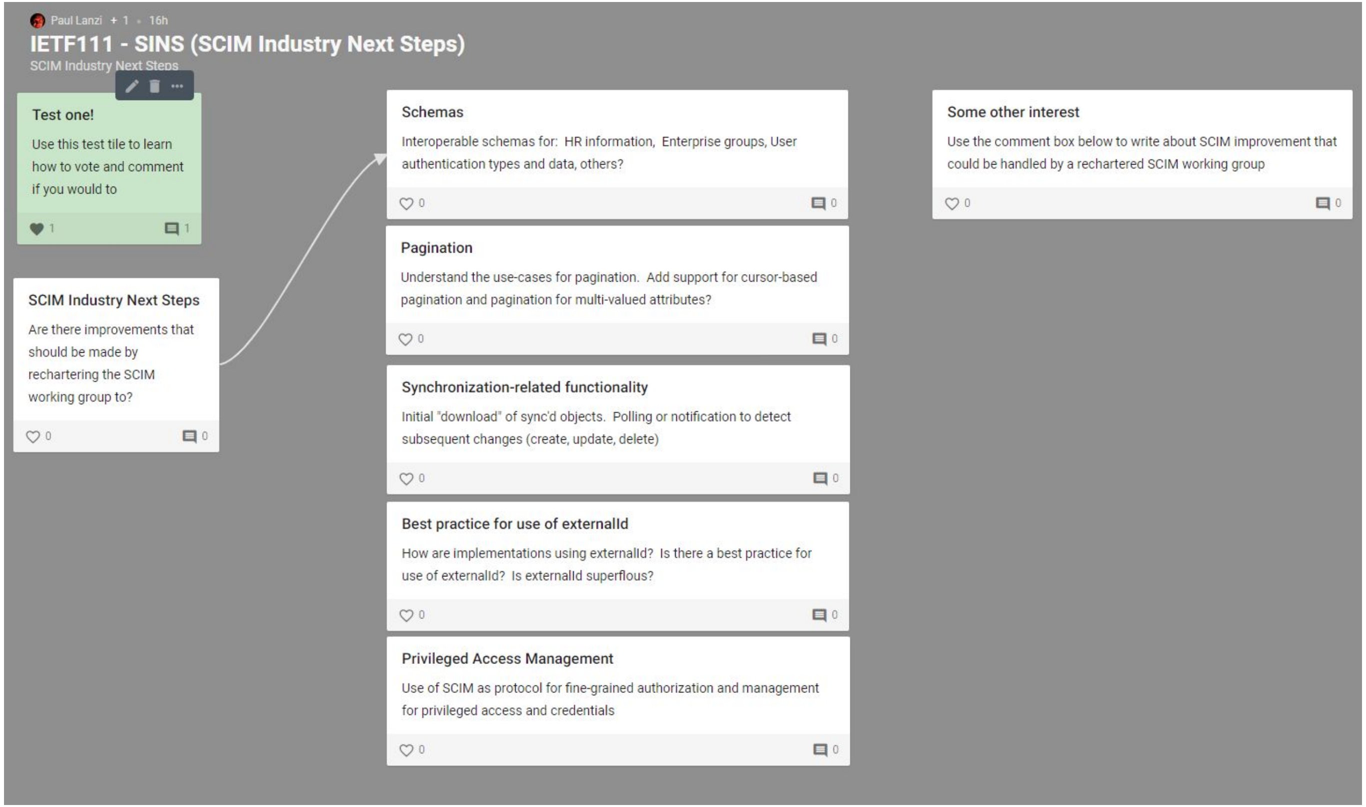

Publish Proposed RFCs

Body of Work - Matt Peterson and Paul Lanzi

Join now:

https://padlet.com/paulpad1/ietf111_sins

Offer votes, comments, suggestions...



Paul Lanzi + 1 • 16h

IETF111 - SINS (SCIM Industry Next Steps)

SCIM Industry Next Steps

Test one!

Use this test tile to learn how to vote and comment if you would to

♥ 1 1

SCIM Industry Next Steps

Are there improvements that should be made by rechartering the SCIM working group to?

♡ 0 0

Schemas

Interoperable schemas for: HR information, Enterprise groups, User authentication types and data, others?

♡ 0 0

Pagination

Understand the use-cases for pagination. Add support for cursor-based pagination and pagination for multi-valued attributes?

♡ 0 0

Synchronization-related functionality

Initial "download" of sync'd objects. Polling or notification to detect subsequent changes (create, update, delete)

♡ 0 0

Best practice for use of externalId

How are implementations using externalId? Is there a best practice for use of externalId? Is externalId superflous?

♡ 0 0

Privileged Access Management

Use of SCIM as protocol for fine-grained authorization and management for privileged access and credentials

♡ 0 0

Some other interest

Use the comment box below to write about SCIM improvement that could be handled by a rechartered SCIM working group

♡ 0 0

Charter Review

https://github.com/SCIM-Interest-Group/wiki/blob/main/WGcharter-firstdraft.md

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

Currently Proposed Charter

https://github.com/SCIM-Interest-Group/wiki/blob/main/WGcharter-firstdraft.md

The System for Cross-domain Identity Management (SCIM) specification is an HTTP-based protocol that makes managing identities in multi-domain scenarios easier. SCIM was last published in 2015 and has seen growing adoption.

One goal for this working group is to shepherd SCIM, currently RFC series 7642, 7643, 7644, through the Internet Standard process. The group will deliver revised specifications for the SCIM requirements as Informational, and for the SCIM protocol and base schema suitable for consideration as a Standard. This work will be based upon the existing RFCs, errata and interoperabilty feedback, and incorporate current security and privacy best practices.

In addition to revising the requirements, protocol and base schema RFCs, the group will also consider additional specifications as extensions to SCIM that have found broad adoption and are ready for standards track. This includes profiles and schemas for interoperability in additional scenarios.

The working group will develop additional Proposed Standard RFCs based on outcomes of the following work:

- Handling returning large result sets through paging, based on draft-hunt-scim-mv-paging-00 and draft-peterson-scim-cursor-pagination-00
- Profiling SCIM for common implementations patterns, based on https://datatracker.ietf.org/doc/html/draft-wahl-scim-profile-00
- Profiling SCIM relationships with other identity-centric protocols such as OAuth 2.0, OpenID Connect, Shared Signals, and Fastfed
- Support for synchronization-related goals between domains
- Evolution of the *externalid* usage
- Handling Deletes in SCIM Servers that don't allow Deletes (Soft Deletes) - based on draft-ansari-scim-soft-delete-00
- Proposals for new Schema definitions
  - Schema for exchanging HR information
  - Schema for exchanging Enterprise group information
  - Schema for Privileged Access Management, based on draft-grizzle-scim-pam-ext-01

How could this Charter unfold?

- Document our modern paradigms
  - Update RFC 7642 (use cases & concepts) to profile proven modern usage patterns & roles
- Determine recommendations for core specification change
  - Security, metadata, interoperability research & implementer feedback
- Schema workshopping
  - One existing proposal, two new proposals
- Extension breakouts
  - Could have impact on core spec change recommendations
- Interop Testing
  - Definitions
  - Events

Next Steps

Thank You!

Connect to the Community

Mailing List:

SCIM Mailing List (ietf.org)

Interest Group Home:

https://github.com/SCIM-Interest-Group

Meeting Calendar (HTML):

https://outlook.live.com/owa/calendar/00000000-0000-0000-0000-000000000000/25ef962b-555f-4781-b533-bfe7be451be8/cid-95C8043F862EFECA/index.html

Meeting Calendar (ICS):

https://outlook.live.com/owa/calendar/00000000-0000-0000-0000-000000000000/25ef962b-555f-4781-b533-bfe7be451be8/cid-95C8043F862EFECA/calendar.ics

SCIM Resources

IETF Datatracker (previous WG)

https://datatracker.ietf.org/wg/scim

Industry Pages

http://simplecloud.info

Implementer Videos

SCIM Fundamentals - Druva

What is SCIM - Okta

Introduction to SCIM - Oracle

Boneyard

Who is using it?

http://www.simplecloud.info/#Implementations2

Logo Slide from Implementations