SCIM Use Cases & Concepts

An analysis of RFC 7642
Facilitator: P. Dingle
IETF 112, 11 November 2021
What is RFC 7642 (https://www.rfc-editor.org/rfc/rfc7642.txt)

Internet Engineering Task Force (IETF)
Request for Comments: 7642
Category: Informational
ISSN: 2070-1721

K. Li, Ed.
Alibaba Group
F. Hunt
Oracle
B. Khasnabish
ZTE (TX) Inc.
A. Nadalin
Microsoft
Z. Zeltsan
Individual
September 2015

System for Cross-domain Identity Management:
Definitions, Overview, Concepts, and Requirements

Abstract

This document provides definitions and an overview of the System for Cross-domain Identity Management (SCIM). It lays out the system’s concepts, models, and flows, and it includes user scenarios, use cases, and requirements.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 7841.

• System for Cross-Domain Identity Management:
  Definitions, Overview, Concepts & Requirements
  Defined 2011-2015
Major Elements

Actors

- Cloud Service Provider
  - CSP
- Enterprise Cloud Subscriber
  - ECS
- Cloud Service User
  - CSU

Figure 1: SCIM Actors
Major Elements

<table>
<thead>
<tr>
<th>Triggers</th>
<th>Modes</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Push</td>
<td>CSP→CSP: Create Identity (Push)</td>
</tr>
<tr>
<td>Update</td>
<td>Pull</td>
<td>CSP→CSP: Update Identity (Push)</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>CSP→CSP: Delete Identity (Push)</td>
</tr>
<tr>
<td>SSO</td>
<td></td>
<td>CSP→CSP: SSO Trigger (Push)</td>
</tr>
</tbody>
</table>

Which one is the Service Provider in RFC 7643 terms?
What if the ECS is the Service Provider? Service providers can’t “push”!
Identity Management has changed in the last 10 years
Hypothesis: Two patterns at the end of the day

- Push & pull often happen together
- Could differ by attribute
- Any participant can either be a client or a Service Provider

Legend
- Primary activity
- Supplemental activity
- Start of Authority (SOA)
Service Provider as Provisioning Hub

SCIM Client → Service Provider → SCIM Client

- **Push** (C.R.U.D.)
  - Eg: update email address

- **Pull**
  - Eg: reconcile data, check before a put/post

A
SCIM Client as Provisioning Hub

- **Service Provider**
  - push (C.R.U.D.)
- **SCIM Client**
  - pull (C.R.U.D.)
  - push
  - Eg: update email address
- **Service Provider**
  - pull
  - Eg: reconcile data, check before a put/post
Multi-Role Data Distribution
Multi-Role Data Distribution

SCIM Client

Service Provider

SCIM Client

Service Provider

SCIM Client

Service Provider

A

push

pull

push

pull

push

push

pull

pull
What could we do in a new draft?

- Define & use in context the terms from RFC 7643/7644
  - Service Provider
  - Client
  - Resource
  - Provisioning Domain
  - Resource Type

- Modernize the Use Cases
  - Multi-directional interactions
  - Ephemeral/time-sensitive uses
  - Large Group management
  - Use of /me
  - Search

- Modernize the Concepts
  - Bi-directionality
  - Start of Authority & data flow
  - Incremental & partial attribute exchange
  - Extensibility & custom schema
  - Synchronization

- Success Criteria
  - Easy to Read
  - Decreases time needed to understand the protocol & schema documents
  - Explains nuance that does not belong in a normative document
Interested?

• Give feedback on direction
• Contact Nancy to volunteer as an Editor
• Help us review drafts

Photo credit: https://flickr.com/photos/51550312@N08/4733445650