SCIM Use cases aka RFC 7642 revamp

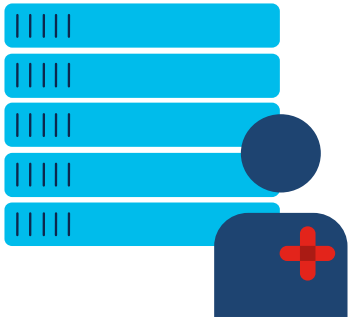
System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements

Pamela Dingle, Paulo Correia

26/Jul/2023

https://github.com/pamelatech/scim-use-case-revamp/blob/main/draft-correia-scimusecases-00.txt

Orchestrator roles

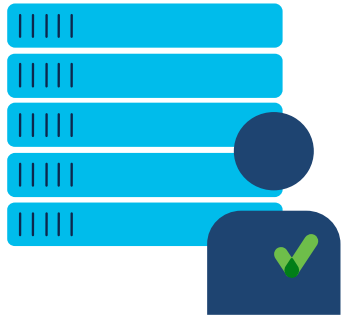


Resource Creator (RC)
Resource Updater (RU)

Component of the system that create/updates the resources and their attributes

Resource Manager (RM)

Component of the system that manage multiple Creators and Subscribers, maintaining the latest information on the resources



Resource Subscriber (RS)

Component of the system that will consume the information from Resource Manager

Orchestrators roles

Resource Object(RO)

Set of attributes for a specific resource, that can contain attributes from multiple Schemas

Resource Attribute (RA)

Single Attribute for a Resources that is specify in one of the schemas of the Resource

Triggers

- Periodic Interval
- Events
- Administrator Actions
- User Actions
- Single SignOn

SCIM Actions

- Create SCIM Identity Resource (Push from RC or RM to RM or RS)
- Update SCIM Identity Resource (Push from RC or RM to RM or RS)
- Delete SCIM Identity Resource (Push from RC or RM to RM or RS)

Push

- Create SCIM Identity Resource (RS or RM Pull from RC or RM)
- Update SCIM Identity Resource (RS or RM Pull from RC or RM)
- Delete SCIM Identity Resource (RS or RM Pull from RC or RM)

Pull

SCIM Use Cases

SCIM Use Cases

/me endpoint CRUD operation on a single resource.

Get information about me, allowing CRUD operation on the user that is authorized to the RS (Service Provider, where the client can only do CRUD operations on the authorized Resource.

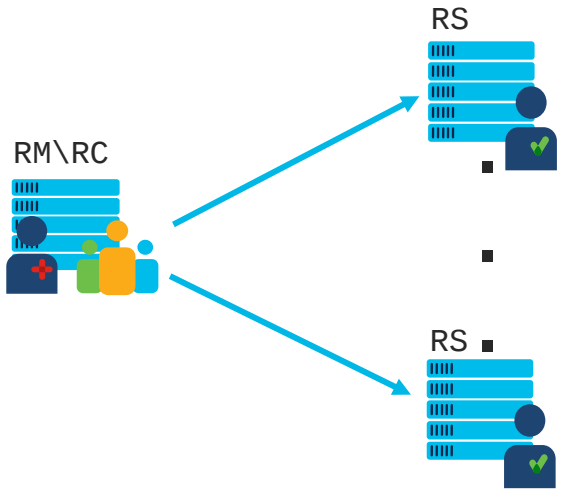
SCIM

RFC 7642

SCIM Use Cases

IdM doing CRUD operations on SaaS applications

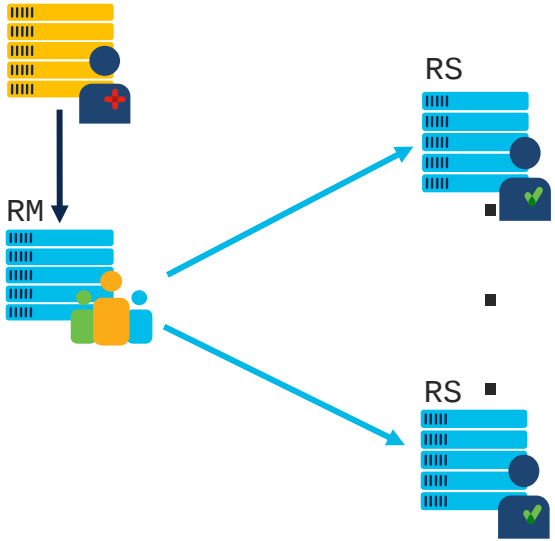
Resources are CUD (Created/Updated/Delete) in the service of RM, manual, bulk or through the use of proprietary APIs, at this point the Actor is a RC and RM
After CUD in RM System, it will be updated in the different RS, where RM will use push to do CUD in specific time intervals.



SCIM Use Cases

IdM doing CRUD operations on SaaS applications, and Objects coming from external non SCIM source

Resources are CUD (Created/Updated/Delete) from an external Identity Engine (typically LDAP source) and add to RM
After CUD in RM system, it will be updated in the different RS, where RM will use push CUD in specific intervals of time.



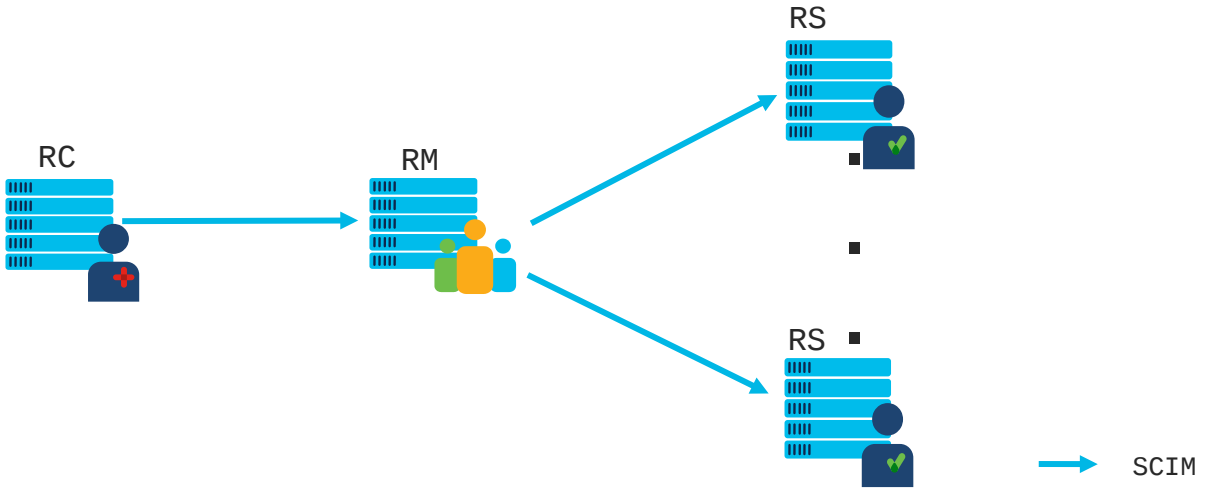
Other protocols like LDAP

SCIM

SCIM Use Cases

IdM doing CRUD operations on SaaS applications, and Objects coming from external SCIM source

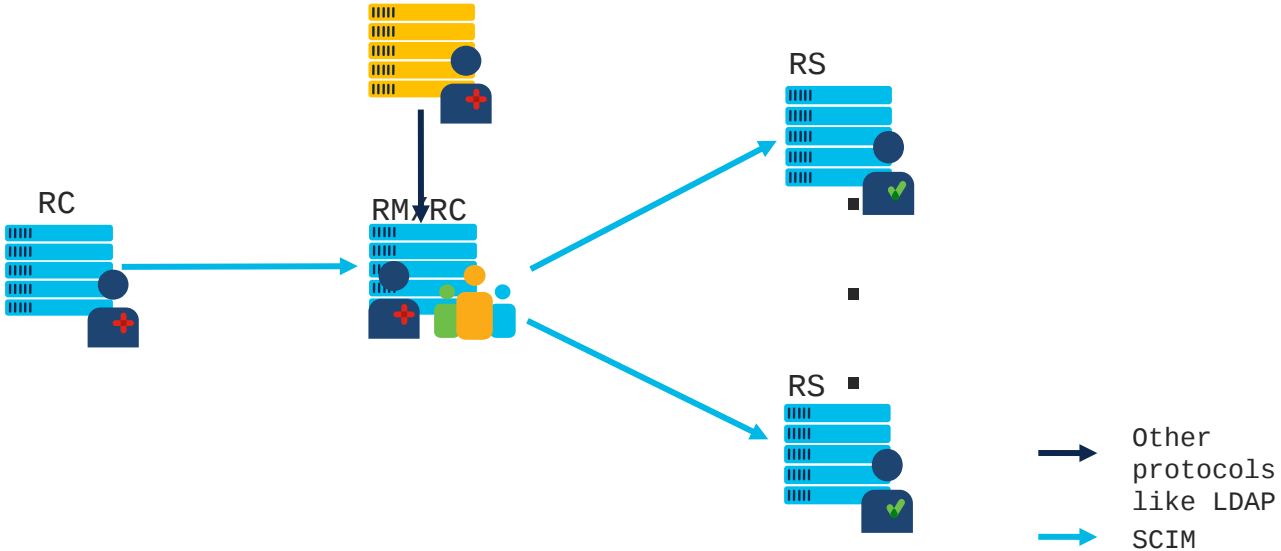
Resources are CUD (Created/Updated/Delete) from an RC (typically an HR applications) to the RM
After CUD in RM system, it will be updated in the different RS, where RM will use push to CUD in specific intervals of time.



SCIM Use Cases

IdM doing CRUD operations on SaaS applications, and Objects coming from external SCIM and non SCIM source including the IDM itself

Resources are CUD (Created/Updated/Delete)from an RC
or from external Identity engine but can also be done locally in the RM.
After CUD in RM system, it will be updated in the different RS, where RM will use push CUD in specific intervals of time.

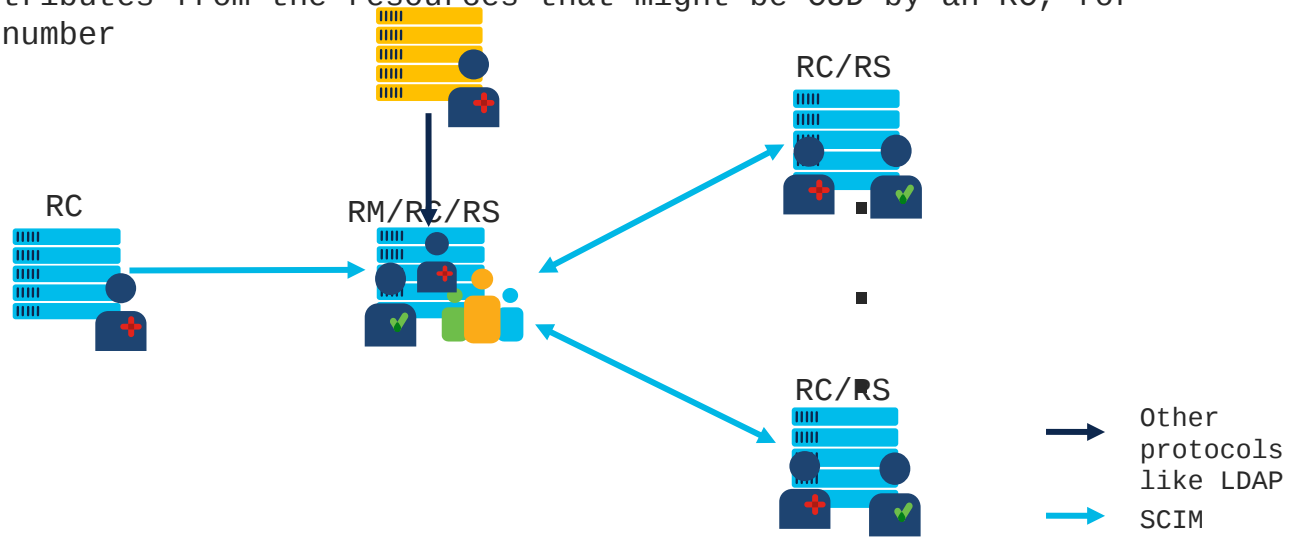


RFC 7642

SCIM Use Cases

IdM doing CRUD operations on SaaS applications, and Objects coming from external SCIM and non SCIM source including the IDM itself, where some object attributes come from SaaS application

Resources are CUD (Created/Updated/Delete)from an RC
or from external Identity engine but can also be done locally in the RM.
After CUD in RM system, it will be updated in the different RS, where RM will use push CUD in specific intervals of time.
There might be some attributes from the resources that might be CUD by an RC, for example the Telephone number

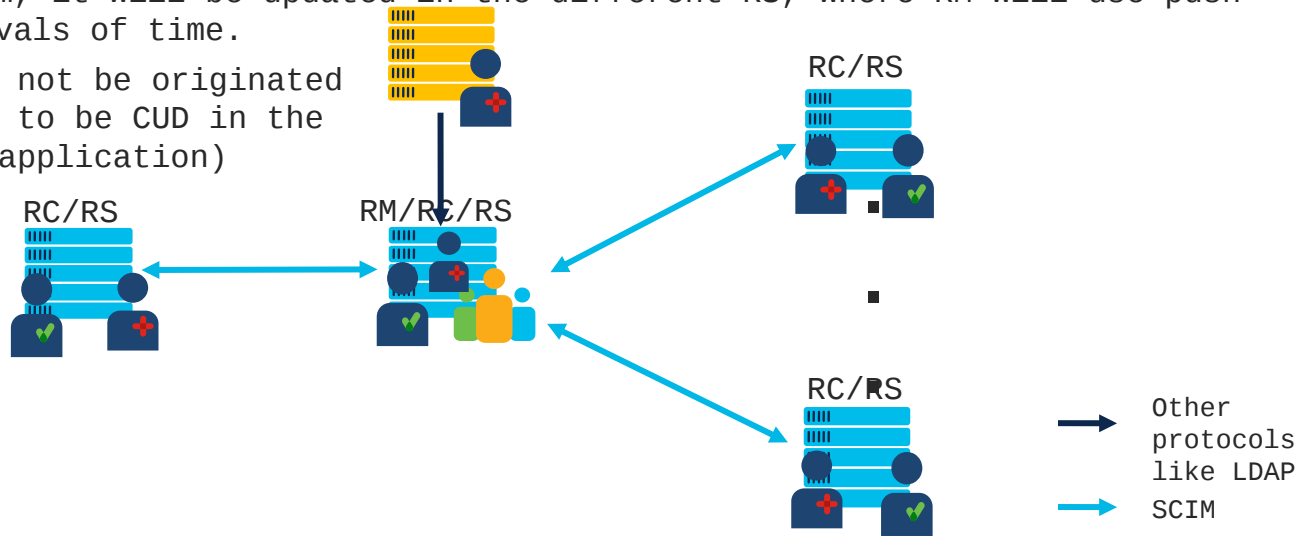


SCIM Use Cases

IdM doing CRUD operations on SaaS applications, and Objects coming from external SCIM and non SCIM sources including the IdM itself, where some object attributes come from SaaS application, and are updated in the SCIM object creator

Resources are CUD (Created/Updated/Delete)from an RC
or from external Identity engine but can also be done locally in the RM.
After CUD in RM system, it will be updated in the different RS, where RM will use push CUD in specific intervals of time.

Attributes that might not be originated in the RC, might need to be CUD in the RC (typically the HR application)



SCIM Use Cases

Multiple IdM doing CRUD operations on SaaS applications, and Objects coming from external SCIM and non SCIM sources including the IdM itself, where some object attributes come from SaaS application, and are updated in the SCIM object creator

Multiple Resource Managers, where the information from the RO/RA is consolidated across different domains/services.