SCIM WG
Internet-Draft
Intended status: Informational
Expires: July 5, 2013

K. Li
Huawei Technologies

Jan 2013

SCIM User Scenarios
draft-li-scim-user-scenarios-00

Abstract

This document lists the user scenarios of System for Cross-domain Identity Management (SCIM).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 5, 2013.

Table of Contents

1. Introduction

This document describes the SCIM user scenarios. The document's objective is to help with understanding of the design and applicability of SCIM schema [I-D.ietf-scim-core-schema] and SCIM protocol [I-D.ietf-scim-api].

The following section provides the abbreviated descriptions of the user scenarios.

2. SCIM User Scenarios

2.1. Background & Context

The Simple Cloud Identity Management (SCIM) specification is designed to make managing user identity in cloud based applications and services easier. The specification suite seeks to build upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models. It's intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence, make it fast, cheap, and easy to move users in to, out of, and around the cloud.

The SCIM user scenarios are overview user stories designed to help clarify the intended scope of the SCIM effort.

2.2. Model Concepts

2.2.1. Triggers

Quite simply, triggers are actions or activities that start SCIM flows. Triggers may not be relevant at the protocol or the schema, they really serve to help identity the type or activity that resulted in a SCIM protocol exchange. Triggers make use of the traditional provisioning C.R.U.D (Create Retrieve Modify & Delete) operations but add additional use case contexts like "SSO" as it is designed to capture a class of use case that makes sense to the actor requesting it rather than to describe a protocol operation.

- Create SCIM Identity Resource - Service On-boarding Trigger: A create SCIM resource trigger is a service on-boarding activity in which a business action such as a new hire or new service subscription is initiated by one of the SCIM Actors. In the protocol itself, service on-boarding may well be implemented via

the same resource PUT method as a service change. This is particular to the implementation not to the use cases that drive that implementation.

- Update SCIM Identity Resource - Service Change Trigger: An Update SCIM resource trigger is a service change activity as a result of an identity moving or changing its service level. An Update Identity trigger might be the result of a change in a service subscription level or a change to key identity data used to denote a service subscription level. Password changes are specifically called out from other more general identity attribute changes as they are considered to have specific use case differences.

- Delete SCIM Identity Resource - Service Termination Trigger: A delete SCIM resource trigger represents a specific and deliberate action to remove an identity from a given SCIM service point. At this stage it is unclear if the SCIM protocol needs to identify separate protocol exchange for a service suspension actions. This may be relevant as target services usually differentiate between these result and may require separate resource representations as a result.

- Single-Sign On (SSO) Trigger - Real-time Service Access Request: A SSO trigger is a special class of activity in which a Create or Update trigger is initiated during an SSO operational flow. The implication here is that as the result of a real-time service access request by the end user (SSO), defined SCIM protocol exchanges can be used to initiate SCIM resource CRUD somewhere in the service cloud.

2.2.2. Actors

Actors are the operating parties that take part in both sides of a SCIM protocol exchange, and help identify the source of a given Trigger. So far, we have identified the following SCIM Actors:

- Cloud Service Provider (CSP): A CSP is the entity operating a given cloud service. In a SaaS scenario this is simply the application provider. In an IaaS or PaaS scenario, the CSP may be the underlying IaaS/PaaS infrastructure provider or the owner of the application running on that platform. In all cases, the CSP is the thing that holds the identity information being operated upon. Put another way, the CSP really is the service that the end-end user interacts with.

- Enterprise Cloud Subscriber (ECS): An ECS represents a middle-tier of aggregation for related identity records. In one of our sample enterprise SaaS scenarios, the ECS is "FooBar.Inc" that subscribes

to a cloud based CRM service "SaaS-CRM.Inc" (the CSP) for all of its sales staff. The actual Cloud Service Users (CSUs) are the FooBar.Inc. sales staff. The ECS actor is identified to help capture use cases in which a single entitle is given administrative responsibility for other identity accounts. SCIM may not address the configuration and setup of an ECS within the CSP, but it does address use cases in which SCIM identity resources are grouped together and administers as part of some broader agreement or operational exchange.

- Cloud Service User (CSU): A CSU represents the real cloud service end-end user - the "person logging into and using the cloud service". As described above, and ECS will typically own or manage multiple CSU identities where as the CSU represents the FooBar.Inc. employee using the cloud service to manage their CRM process.

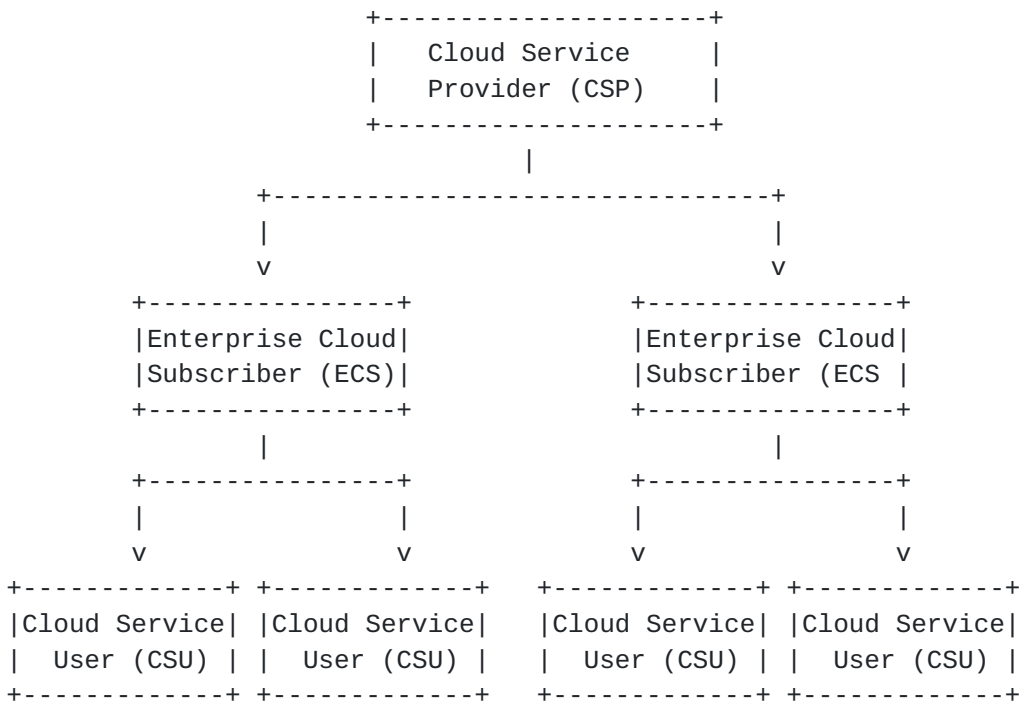

Figure 1: SCIM Actors

2.2.3. Modes & Flows

Modes identify the functional intent of a data-flow initiated in a SCIM scenario. The modes identified so far are 'push' and 'pull' referring to the fact of pushing data to, or pulling data from an authoritative identity data store.

In the SCIM scenarios, Modes are often used in the context of a flow between two Actors. For example, one might refer to a Cloud-to-Cloud Pull exchange. Here one Cloud Service Provider (CSP) is pulling identity information from another CSP. Commonly referenced flows are:

- Cloud Service Provider to Cloud Service Provider (CSP->CSP)
- Enterprise Cloud Subscriber to Cloud Service Provider (ECS-CSP)

Modes & flows simply help us understand what is taking place; they are likely to be technically meaningless at the protocol level, but again they help the reader follow the SCIM scenarios and apply them to real work use cases.

2.2.4. Bulk & Batch Operational Semantics

It is assumed that each of the triggers action outlined in this document may be part of the larger bulk or batch operation. Individual SCIM actions should be able to be collected together to create single protocol exchanges.

The initial focus of SCIM scenarios is on identifying base flows and single operations. The specific complexity of full bulk and batch operations is left to a later version of the scenarios or to the main specification.

2.3. Cloud Service Provider to Cloud Service Provider Flows (CSP->CSP)

These scenarios represent flows between two Cloud Service Providers (CSPs). It is assumed that each CSP maintains an Identity Data Store for its Cloud Service Users (CSUs). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the CSPs.

2.3.1. CSP->CSP - Create Identity (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Create Identity trigger action from its Enterprise Cloud Subscriber (ECS-1). CSP-1 creates a local user account for the new CSU. CSP-1 then pushes the new CSU joiner push request down-stream to CSU-2 and gets confirmation that the account was successfully created. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgement to the requesting ECS.

2.3.2. CSP->CSP - Update Identity (Push)

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. The Enterprise Cloud Subscriber (ECS-1) has already created an account with CSP-1 and supplied a critical attribute "department" that is used by CSP-1 to drive service options. CSP-1 then receives an Update Identity trigger action from its Enterprise Cloud Subscriber (ECS). CSP-1 updates its local directory account with the new department value. CSP-1 then initiates a separate SCIM protocol exchange to push the mover change request down-stream to CSP-2. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgment to ECS-1.

2.3.3. CSP->CSP - Delete Identity (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Delete Identity trigger action from its Enterprise Cloud Subscriber (ECS-1). CSP-1 suspends the local directory account for the specified CSU account. CSP-1 then pushes a termination request for the specified CSU account down-stream to CSP-2 and gets confirmation that the account was successfully removed. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgment to the requesting ECS.

This use case highlights how different CSPs may implement different operational semantics behind the same SCIM operation. Note CSP-1 suspends the account representation for its service where as CPS-2 implements a true delete operation.

2.3.4. CSP->CSP - SSO Trigger (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-1 waits for a service access request from the end Cloud Service User (CSU-1) before issuing account creation details to CSP-2. When the CSU completes a SSO transaction from CSP-1 to CSP-2, CSP-2 then creates an account for the CSU based on information pushed to it from CSP-1.

At the protocol level, this class of scenarios may result in the use of common protocol exchange patters between CSP-1 & CSP-2.

2.3.5. CSP->CSP - SSO Trigger (Pull)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-2 waits for a service access request from the Cloud Service User (CSU-1) before initiating a Pull request to gather information about the CSU sufficient to create a local account.

At the protocol level, this class of scenarios may result in the use of common protocol exchange patterns between CSP-2 & CSP-1.

2.3.6. CSP->CSP - Password Reset (Push)

In this scenario two CSPs (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 wants to change the password for a specific Cloud Service User (CSU-1). CSP-1 sends a request to CSP-2 to reset the password value for CSU-1.

At the protocol level, this scenario may result in the same protocol exchange as any other attribute change request.

2.4. Enterprise Cloud Subscriber to Cloud Service Provider Flows(ECS->CSP)

These scenarios represent flows between an Enterprise Cloud Subscriber (ECS) and a Cloud Service Providers (CSP). It is assumed that both the ECS and the CSP maintains an LDAP service for the relevant Cloud Service Users (CSUs). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the ECS and the CSP.

Many of these scenarios are very similar to those defined in the Cloud Service Provider to Cloud Service Provider section above. They are identified separately here so that we may explore any differences and might emerge.

2.4.1. ECS->CSP - Create Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1) that requires the sharing of various Cloud Service User (CSU) accounts. A new user joins ECS-1 and so ECS-1 pushes an account creation request to CSP-1, supplying all required base SCIM schema attribute values and additional extended SCIM schema values as required.

2.4.2. ECS ->CSP - Update Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with Cloud Service Provider (CSP-1) that drives service definition from a key account schema attribute called Department. ECS-1 wishes to move a given CSU from Department A to Department B and so it pushes an attribute update request to the CSP.

2.4.3. ECS ->CSP - Delete Identity (Push)

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). Upon termination of one of its employees' employment agreement, ECS-1 sends a suspend account request to CSP-1 (Figure 1.4.3-1). One week later the ECS wishes to complete the process by fully removing the Cloud Service User (CSU) account and so it sends a terminate account request to CSP-1.

2.4.4. ECS ->CSP - SSO Pull

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). No accounts are created or exchanged in advance. However, rather than pre-provisioning accounts from ECS-1 to CSP-1, CSP-1 waits for a service access request from the Cloud Service User (CSU-1) under the control domain of ECS-1, before issuing an account Pull request to CSP-1.

3. Recommendations

The recommendation is to merge the user scenarios document into the use case document as section 2.

4. Security considerations

TBD

5. IANA considerations

This Internet Draft includes no request to IANA.

6. Acknowledgements

Authors would like to thank Darran Rolls and Patrick Harding, most of the texts in this document are taken from them.

Thanks to Bert Greevenbosch for his review and feedback.

7. Informative References

[I-D.ietf-scim-api]
Drake, T., Mortimore, C., Ansari, M., Grizzle, K., and E. Wahlstroem, "System for Cross-Domain Identity Management: Protocol", draft-ietf-scim-api-00 (work in progress), August 2012.

[I-D.ietf-scim-core-schema]
Mortimore, C., Harding, P., Madsen, P., and T. Drake, "System for Cross-Domain Identity Management: Core Schema", draft-ietf-scim-core-schema-00 (work in progress), August 2012.

Author's Address

Kepeng LI
Huawei Technologies
Bantian
Shenzhen, Guangdong 518129
China

Email: likepeng@huawei.com