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

K. LI, Ed.
Alibaba Group
P. 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 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7642.

Table of Contents

1. Introduction

This document provides the SCIM definitions, overview, concepts, flows, scenarios, and use cases. It also provides a list of the requirements derived from the use cases.

The document's objective is to help with understanding of the design and applicability of the SCIM schema [RFC7643] and SCIM protocol [RFC7644].

Unlike the practice of some protocols like Application Bridging for Federated Access Beyond web (ABFAB) and SAML2 WebSSO, SCIM provides provisioning and de-provisioning of resources in a separate context from authentication (aka just-in-time provisioning).

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. These words may also appear in this document in lowercase as plain English words, absent their normative meanings.

Here is a list of acronyms and abbreviations used in this document:

- COI: Community of Interest
- CRM: Customer Relationship Management
- CRUD: Create, Read, Update, Delete
- CSP: Cloud Service Provider
- CSU: Cloud Service User
- ECS: Enterprise Cloud Subscriber
- IaaS: Infrastructure as a Service
- JIT: Just In Time
- PaaS: Platform as a Service
- SaaS: Software as a Service
- SAML: Security Assertion Markup Language

- SCIM: System for Cross-domain Identity Management
- SSO: Single Sign-On

2. SCIM User Scenarios

2.1. Background and Context

The System for Cross-domain Identity Management (SCIM) specification is designed to manage user identity in cloud-based applications and services in a standardized way to enable interoperability, security, and scalability. 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. The intent of the SCIM specification 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 scenarios are overviews of 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 level or the schema level; they really serve to help identify the type or activity that resulted in a SCIM protocol exchange. Triggers make use of the traditional provisioning CRUD (Create, Read, Update, Delete) operations but add additional use-case contexts like SSO (Single-Sign On) 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 identity 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, and not to the use cases that drive that implementation.

- Update SCIM Identity Resource - Service Change Trigger: An "update SCIM identity resource" trigger is a service change activity as a result of an identity moving or changing its service level. An "update SCIM 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 identity 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 a separate protocol exchange for service suspension actions. This may be relevant as target services usually differentiate between these results and thus may require separate resource representations.

- Single Sign-On (SSO) Trigger - Service Access Request: A "Single Sign-On" 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 service access request by the end user (SSO), defined SCIM protocol exchanges can be used to initiate SCIM resource CRUD operations 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 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 "Example.com" 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 entity 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 administered as part of some broader agreement or operational exchange.

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

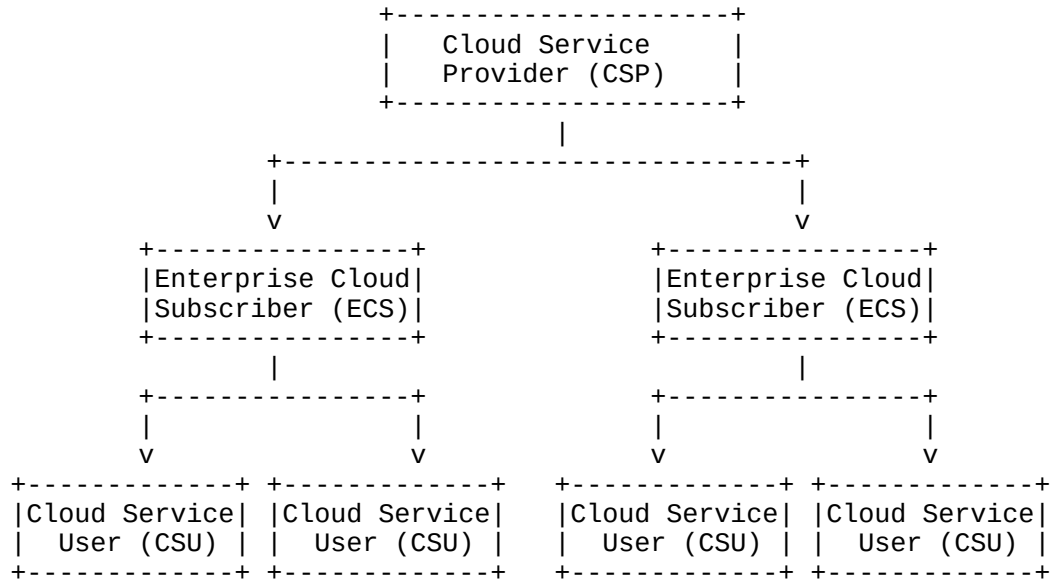

Figure 1: SCIM Actors

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

2.2.4. Bulk and Batch Operational Semantics

It is assumed that each of the trigger actions 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. Flows from Cloud Service Provider to Cloud Service Provider (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 and 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 downstream to CSU-2 and gets confirmation that the account was successfully created. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgment to the requesting ECS.

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

In this scenario, two CSPs (CSP-1 and 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 downstream 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 and 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 downstream to CSP-2 and gets confirmation that the account was successfully removed. After receiving the confirmation from CSP-2, CSP-1 finalizes the deletion operation and 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, whereas CPS-2 implements a true delete operation.

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

In this scenario, two CSPs (CSP-1 and 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 patterns between CSP-1 and CSP-2.

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

In this scenario, two CSPs (CSP-1 and 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 and CSP-1.

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

In this scenario, two CSPs (CSP-1 and 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. Flows from Enterprise Cloud Subscriber to Cloud Service Provider (ECS->CSP)

These scenarios represent flows between an Enterprise Cloud Subscriber (ECS) and a Cloud Service Providers (CSP). It is assumed that the ECS and the CSP each maintain an information access 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 Section 2.3. They are identified separately here so that we may explore any differences that 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 attribute values for the base SCIM schema and additional values for the extended SCIM schema 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 employee's employment agreement, ECS-1 sends a suspend account request to CSP-1. One week later, the ECS wishes to complete the process by fully removing the Cloud Service User (CSU) account, so it sends a terminate account request to CSP-1.

2.4.4. ECS->CSP: SSO Trigger (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 ECS-1.

3. SCIM Use Cases

This section lists the SCIM use cases.

3.1. Migration of the Identities

Description:

A company SomeEnterprise runs an application ManageThem that relies on the identity information about its employees (e.g., identifiers, attributes). The identity information is stored at the cloud provided by SomeCSP. SomeEnterprise has decided to move identity information to the cloud of a different provider -- AnotherCSP. In addition, SomeEnterprise has purchased a second application ManageThemMore, which also relies on the identity information. SomeEnterprise is able to move identity information to AnotherCSP without changing the format of identity information. The application ManageThemMore is able to use the identity information.

Pre-conditions:

- SomeCSP is a cloud service provider for SomeEnterprise.

- SomeCSP has a known attribute name and value for the Enterprise used for managing and transferring data.

- AnotherCSP is a new cloud service provider for SomeEnterprise.

- All involved cloud service providers and applications support the same standard specifying the format for and actions on the user (e.g., employee) identity information.

Post-conditions:

- SomeEnterprise has moved its employees' identity information from SomeCSP to AnotherCSP without making any changes to representation of identity information.

- Application ManageThemMore is able to use the identity information.

Requirements:

- SomeEnterprise, the applications ManageThem and ManageThemMore, and the providers SomeCSP and AnotherCSP support a common standard for identity information, which specifies the following:

  * Format (or schema) for representing user identity information

  * Interfaces and protocol for managing user identity information

- Cloud providers shall be able to meet regulatory requirements when migrating identity information between jurisdictional regions (e.g., countries and states may have differing regulations on privacy).

- Cloud providers shall be able to log all actions related to SomeEnterprise employees' identities.

- The logs should be secure and available for auditing.

3.2. Single Sign-On (SSO) Service

Description:

Bob has an account in an application hosted by a cloud service provider SomeCSP. SomeCSP has federated its user identities with a cloud service provider AnotherCSP. Bob requests a service from an application running on AnotherCSP. The application running on AnotherCSP, relying on Bob's authentication by SomeCSP and using identity information provided by SomeCSP, serves Bob's request.

Pre-conditions:

- Bob’s identity information is stored on SomeCSP.
- SomeCSP and AnotherCSP have established trust and federated their user identities.
- SomeCSP is able to authenticate Bob.
- SomeCSP is able to securely provide the authentication results to AnotherCSP.
- SomeCSP is able to securely provide Bob’s identity information (e.g., attributes) to AnotherCSP.
- AnotherCSP is able to verify information provided by SomeCSP.
- SomeCSP is able to process the identity information received from AnotherCSP.

Post-conditions:

Bob has received the requested service from an application running on AnotherCSP without having to authenticate to that application explicitly.

Requirements:

- Bob must have an account with SomeCSP.
- SomeCSP and AnotherCSP must establish trust and federate their user identities.
- SomeCSP must be able to authenticate Bob.
- SomeCSP must be able to securely provide the authentication results to AnotherCSP.
- SomeCSP must be able to securely provide Bob’s identity information (e.g., attributes) to AnotherCSP.
- AnotherCSP must be able to verify the identity information provided by SomeCSP.
- SomeCSP must be able to process the identity information received from AnotherCSP.

- SomeCSP and AnotherCSP must log information generated by Bob's actions according to their policies and the trust agreement between them.

3.3. Provisioning of the User Accounts for a Community of Interest (COI)

Description:

Organization YourHR provides Human Resources (HR) services to a Community of Interest (COI) YourCOI. The HR services are offered as Software as a Service (SaaS) on public and private clouds. YourCOI's offices are located all over the world. Their Information Technology (IT) systems may be composed of combinations of the applications running on private and public clouds along with traditional IT systems. The local YourCOI offices are responsible for collecting personal information (i.e., user identities and attributes). YourHR services provide means for provisioning and distributing the employee identity information across all YourCOI offices. YourHR also enables individual users (e.g., employees) to manage personal information that they are responsible for (e.g., update of an address or a telephone number).

Pre-conditions:

- YourCOI has a complex infrastructure composed of a large number of local offices that rely on diverse IT systems.
- YourCOI has contracted YourHR to provide the HR services.
- Each local office has a right to establish a personal account for an employee.

Post-conditions:

- All personal accounts are globally available to any authorized user or application across the YourCOI system through the services provided by YourHR.
- The employees have the ability to manage the part of personal information that is their responsibility.

Requirements:

- YourHR must ensure that the local offices generate information that is provisioned securely and consider privacy requirements in a timely fashion across systems that may span technical (e.g., protocols and applications), administrative (e.g., corporate), regulatory (e.g., location), and jurisdictional domains.

- Management of personal information must be protected against unauthorized access and eavesdropping, and it should be distributed only to authorized parties and services.

- Regulatory requirements shall be met when migrating identity information between jurisdictional regions (e.g., countries and states may have differing regulations on privacy).

- All operations with identity data must be securely logged.

- The logs should be available for auditing.

3.4. Transfer of Attributes to a Relying Party's Website

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits the website of relying party B, and the website requires attributes of the user. The user selects some attributes and authorizes the transfer of data via authorization protocols (e.g., OAuth, SAML), so selected attributes of the user are transferred from the user's account in directory service A to the website of replying party B at the time of the user's first visit to that site.

Pre-conditions:

- User has an account in directory service A.

- User has one or more attributes.

- User visits website of relying party B.

Post-conditions:

Selected attributes of the user are transferred from the user's account in directory service A to the website of relying party B at the time of the user's first visit to that site.

Requirements:

- Relying party B must be able to authenticate the end user.
- Relying party B must be able to securely provide the authentication results to directory service A.
- Directory service A must be able to securely provide end user's identity information (e.g., attributes) to relying party B.
- Regulatory requirements shall be met when migrating identity information between jurisdictional regions (e.g., countries and states may have differing regulations on privacy).
- Relying parties have to be aware of changes to their cached copy, as these would potentially cause a state change in other relying parties.
- A maximum period should be set for the relying party to cache the information.

3.5. Change Notification

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits the web site of relying party B. The website of relying party B queries directory service A for attributes associated with that user, and related resources.

The attributes of the user change later in directory service A. For example, the attributes might change if the user changes their name, has their account disabled, or terminates their relationship with directory service A. Furthermore, other resources and their attributes might also change. The directory service A then wishes to notify the website of relying party B of these changes, as relying party B might (or might not) have a cache of those attributes, and if relying party B were aware of these changes to their cached copy, it would potentially cause a state change in relying party B.

The volume of changes, however, might be substantial, and only some of the changes may be of interest to relying party B, so directory service A does not wish to "push" all the changes to B. Instead, directory service A wishes to notify B that there are changes potentially of interest, such that B can at an appropriate time subsequently contact directory service A and retrieve just the subset of changes of interest to B.

Note that the user must authorize directory service A to transfer data to the website, and the user must authorize directory service A to notify the website.

Pre-conditions:

- User has an account in directory service A.
- User has one or more attributes.
- User visits the website of relying party B.
- The resource being updated is at the website.

Post-conditions:

Directory service A is able to notify relying party B that there are changes potentially of interest.

Requirements:

- Relying party B must be able to authenticate the end user.
- Relying party B must be able to securely provide the authentication results to directory service A.
- Directory service A must be able to securely provide end user's changed identity information (e.g., attributes) to relying party B.
- Relying party B must be able at an appropriate time to subsequently contact directory service A and retrieve just the subset of changes of interest to relying party B.

4. Security Considerations

Authentication and authorization must be guaranteed for the SCIM operations to ensure that only authenticated entities can perform the SCIM requests and the requested SCIM operations are authorized.

SCIM resources (e.g., Users and Groups) can contain sensitive information. Thus, data confidentiality MUST be guaranteed at the transport layer.

There can be privacy issues that go beyond transport security, e.g., moving personally identifying information (PII) offshore between CSPs. Regulatory requirements shall be met when migrating identity information between jurisdictional regions (e.g., countries and states may have differing regulations on privacy).

Additionally, privacy-sensitive data elements may be omitted or obscured in SCIM transactions or stored records to protect these data elements for a user. For instance, a role-based identifier might be used in place of an individual’s name.

Detailed security considerations are specified in Section 7 of the SCIM protocol [RFC7644] and Section 9 of the SCIM schema [RFC7643].

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

5.2. Informative References

[RFC7643] Hunt, P., Ed., Grizzle, K., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Core Schema", RFC 7643, DOI 10.17487/RFC7643, September 2015, <http://www.rfc-editor.org/info/rfc7643>.

[RFC7644] Hunt, P., Ed., Grizzle, K., Ansari, M., Wahlstroem, E., and C. Mortimore, "System for Cross-domain Identity Management: Protocol", RFC 7644, DOI 10.17487/RFC7644, September 2015, <http://www.rfc-editor.org/info/rfc7644>.

Acknowledgments

The authors would like to thank Ray Counterman, Richard Fiekowsky, Bert Greevenbosch, Barry Leiba, Kelly Grizzle, Magnus Nystrom, Stephen Farrell, Kathleen Moriarty, Benoit Claise, Dapeng Liu, and Jun Li for their reviews and comments.

Also, thanks to Darran Rolls and Patrick Harding; Section 2 ("SCIM User Scenarios") is taken from them.

Authors' Addresses

Kepeng LI (editor)
Alibaba Group
969 Wenyixi Road, Yuhang District
Hangzhou, Zhejiang 311121
China

Email: kepeng.lkp@alibaba-inc.com

Phil Hunt
Oracle

Email: phil.hunt@oracle.com

Bhumip Khasnabish
ZTE (TX) Inc.
55 Madison Ave, Suite 302
Morristown, New Jersey 07960
United States

Phone: +001-781-752-8003
Email: vumip1@gmail.com, bhumip.khasnabish@ztetx.com
URI: http://tinyurl.com/bhumip/

Anthony Nadalin
Microsoft

Email: tonynad@microsoft.com

Zachary Zeltsan
Individual

Email: Zachary.Zeltsan@gmail.com