

# SCIM Notify Draft

IETF 92

March 2015

Phil Hunt, Ian Glazer, Morteza Ansari

# IETF NOTEWELL

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session

The IESG, or any member thereof on behalf of the IESG

Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices

Any IETF working group or portion thereof

Any Birds of a Feather (BOF) session

The IAB or any member thereof on behalf of the IAB

The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

# Agenda

- Introduction
- Draft-hunt-scim-notify
  - Event Types
  - Event Messages
  - Notification Hub
  - Publisher and Subscriber Endpoints
- Discussion

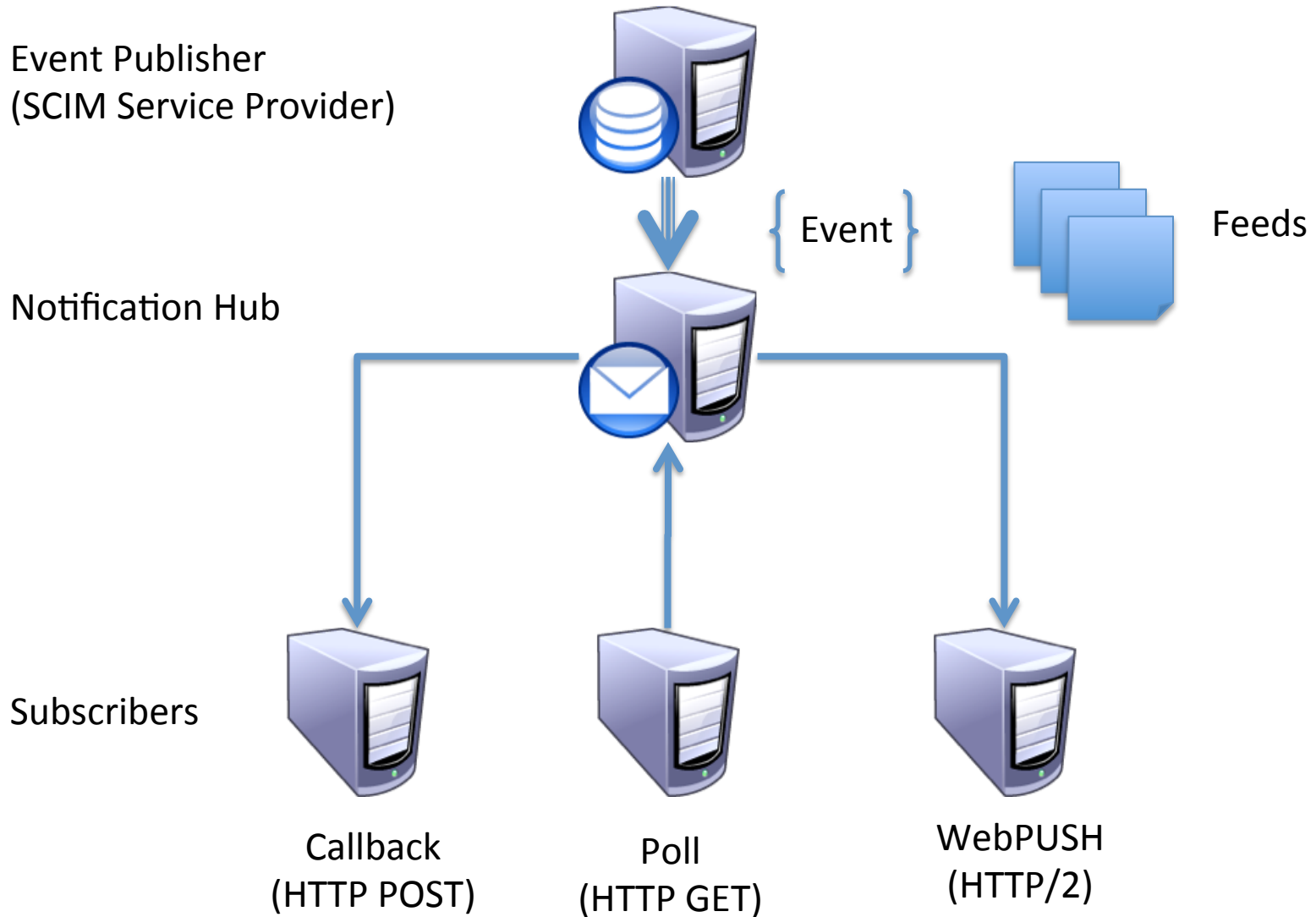
# Introduction

- The original Use Case document describes triggers and protocol  
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 identify the type or activity that resulted in a SCIM protocol exchange. Triggers make use of the traditional provisioning C.R.U.D (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.
- Notify is a way to communicate triggers between publishers and subscribers that can activate SCIM Protocol requests.

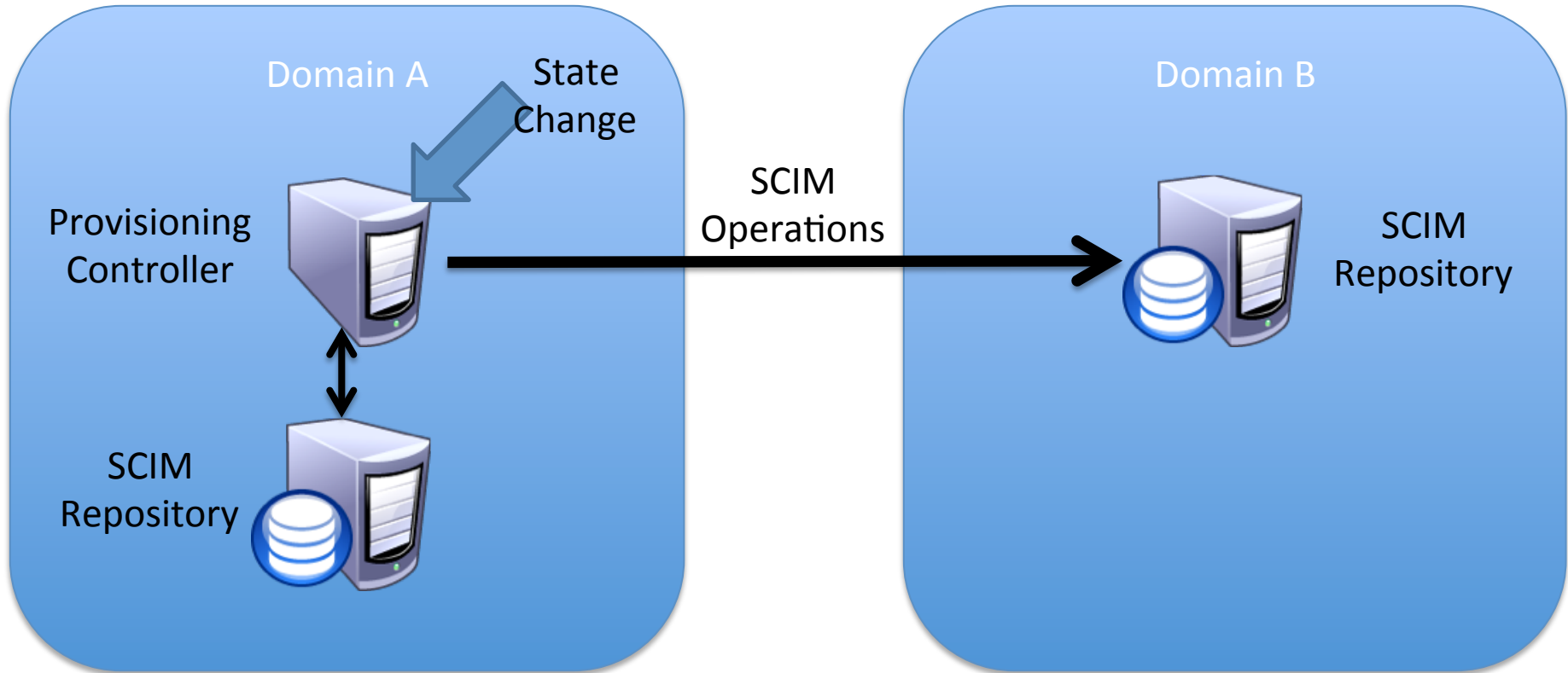
# More Generally...

- A way to notify external domains about changes in state for a set of resources
- A way to notify mobile apps about profile changes
- Enable SCIM service providers to
  - Co-ordinate workflow events with enterprise internal IDM systems
  - Co-ordinate events cross-cloud between providers/tenancies

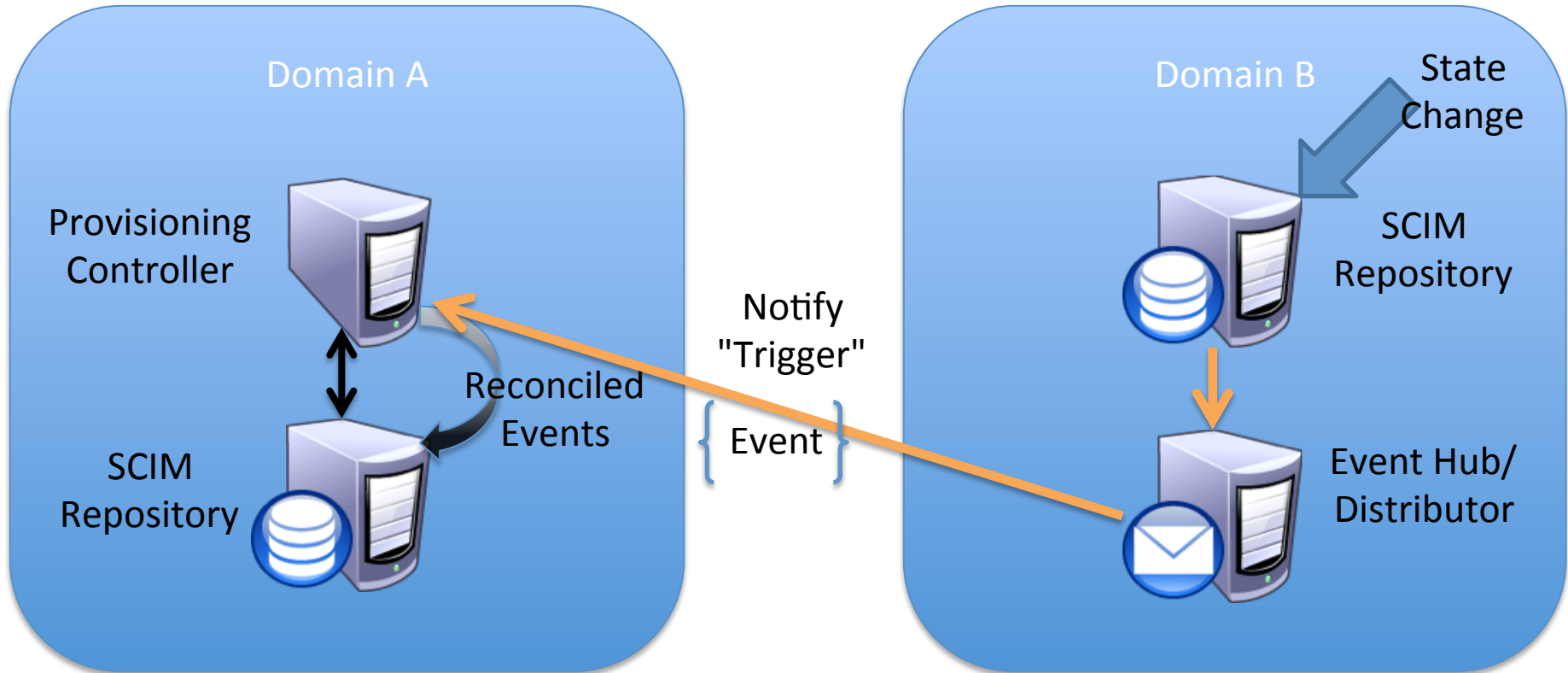
# Architecture



# Typical SCIM



# Events





# Proposed Event Types

- ADD/REMOVE – A resource was added/remove to/from the feed
- CREATE – A resource was created
- ACTIVATE/DEACTIVATE – A resource is enabled/disabled
- MODIFY – A resource has been modified
- DELETE – A resource was deleted
- PASSWORD – Password change
- CONFIRMATION – Used for subscription verification
- Note: we may want to refine/reduce this list

# Published Event Message

```
{
  "schemas":["urn:ietf:params:scim:schemas:notify:2.0:Event"],
  "publisherUri":"https://scim.example.com",
  "feedUris":[
    "https://jhub.example.com/Feeds/98d52461fa5bbc879593b7754",
    "https://jhub.example.com/Feeds/5d7604516b1d08641d7676ee7"
  ],
  "resourceUris":[
    "https://scim.example.com/Users/44f6142df96bd6ab61e7521d9"
  ],
  "type":"CREATE",
  "attributes":["id","name","userName","password","emails"],
  "values":{
    "emails":[
      {"type":"work","value":"jdoe@example.com"}
    ],
    "password":"not4u2no",
    "userName":"jdoe",
    "id":"44f6142df96bd6ab61e7521d9",
    "name":{
      "givenName":"John",
      "familyName":"Doe"
    }
  }
}
```



# Discussion

- Question: Does the working group want to adopt Notify as a WG item?