INTERNET-DRAFT P. Hunt
Intended Status: Proposed Standard Oracle
Expires: March 10, 2013 K. Grizzle
Sailpoint
September 6, 2012

SCIM Targeted Resource Extension
draft-hunt-scim-targeting-01

Abstract

The core SCIM 1.0 specification is intended to provide updates to a single cloud-based application. This extension specifies an extended API definition which allows a single SCIM endpoint to support updates to multiple cloud-based applications. These extensions enable network relationships such as proxy updates, and hub-to-hub-to-spoke relationships in addition to the hub-spoke relationship defined in the core SCIM 1.0 specification.

Status of this Memo

Copyright and License Notice

Table of Contents

1 Introduction

This specification extends the SCIM Protocol [draft-scim-api-00] and [draft-scim-core-schema-00] to enable a SCIM service endpoint to act as a 'gateway' to process requests intended for other connected cloud services called 'targets'. A gateway is essentially a proxy that front-ends one or more applications for the purpose of provisioning. The gateway may act as a simple proxy, or it may act as a hub storing data to be used directly or indirectly by other cloud systems. A 'target' is a logical representation of a remotely connected system to be provision. Such a system may be in-turn, connected via SCIM or some other API supported by the gateway node. The targeting extension is intended to support all SCIM operations and layers on top of SCIM 1.0.

The target resource extensions allow requesting clients to make updates to entities within the gateway itself and additionally, updates to be routed by the gateway to specific target end-points.

```
                                      +----------+
                                      |CRM Target|
                                      +--+-------+
                                         |
             +------+          +-------+---+
             |Client|--------->|Gateway/Hub|
             +------+          +-------+---+
                                         |
                                     +---+--------+
                                     |Email Target|
                                     +------------+
```

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 RFC 2119 [RFC2119].

2. Service Provider Types The following non-normative section describes 3 different types of service providers to illustrate how SCIM

Resource Targeting may be used. With resource targeting, SCIM service providers are broken into 3 types: Spoke, Hubs, and Gateways. Each service provider has different capabilities and are used together to form a complete provisioning infrastructure.

2.1 Spoke Service Provider A spoke service provider is a SCIM service provider where accounts are to be provisioned using the SCIM 1.0

APIs. It usually represents a single logical repository of identities.

2.2 Hub Service Provider A hub service provider offers the same features of a spoke, but it can also provision resources to connected service providers known as "targets". A "target" is a SCIM service provider that implements SCIM protocol or another protocol in such a way that it appears to accept SCIM transactions. Resources stored in the hub can be associated with "target" provisioned resources through the use of a complex attribute "accountRefs" which links hub resources to resources in target service providers.

2.3 Gateway Service Provider A gateway is similar to a SCIM hub except that it has no local repository and is therefore stateless. Typically a gateway is used as an architectural component to firewall direct access to individual SCIM Service Provider endpoints by allowing transactions to flow through a common gateway.

3. Extended Resource API

The SCIM protocol specifies well known endpoints and HTTP methods for managing Resources defined in the core schema such as User and Group resources. The core schema defines key Relative Resource URLs which can be used to perform SCIM operations.

In addition to the endpoints defined in section 3 of [draft-scim-api-00], the following endpoints are defined:

3.1 Local Endpoints

In SCIM 1.0, all operations are presumed to occur on the current end-point. SCIM Hub and Gateway servers have additional server endpoints that enable discovery of Target entities where transactions can be routed.

/Targets
[Operations: GET]
Use in GET operations to retrieve a list of logical target entities available within the current SCIM server. The information can be used by the client to discover provisioning end-points accessible via the current SCIM service provider.

/Targets/{target_id}
[Operations: GET]
Use in GET operations to retrieve information about a particular Target identified by {target_id}.

3.2 Targeted Operations

Targeting extends the SCIM protocol so that SCIM operations can be

routed to a logical server. Targeting adds a prefix to the endpoint path to all normal SCIM operations as follows.

/Targets/{target_id}/{scim-endpoint-url}
[Operations: All]

This general pattern indicates that a transaction is to be routed to a target identified by {target_id}. {scim-endpoint-url} is any valid SCIM 1.0 relative endpoint URL. The routed operation MAY in turn be another SCIM protocol call. However it MAY ALSO be over a different protocol as long as it behaves within the hub or gateway as a SCIM operation.

For example:
/Targets/crm/Users/2819c223-7f76-453a-919d-413861904646

/Targets/{target_id}/ServerProviderConfigs
[Operations: Get]

Retrieves the service provider configuration of the target identified by the logical target identifier {target_id}. Included in the server configuration MAY be the 'type' attribute which specifies the server type of 'spoke', 'gateway', or 'hub' and defaults to 'spoke'. If target communication is not via SCIM, the target 'connector' should behave as if it was. The ServerProviderConfig returned SHOULD reflect the real SCIM endpoint configuration, or the equivalent if SCIM protocol is not used to connect the Target Service Provider.

/Targets/{target_id}/Schemas
[Operations: Get]

Retrieves the targeted service provider's schema. The schema returned should reflect the Target Service Provider's schema or the equivalent if SCIM protocol is not used to connect the Target Service Provider.

/Targets/{target_id}/Users
/Targets/{target_id}/Groups
[Operations: All]

Retrieves/updates the User or Group entities from {target_id} as if the request was sent directly to {target_id}.

/Targets/{target_id}/Users/{user_id}'
[Operations: All]

References the User entity {user_id} within the Target identified by {target_id}.

/Targets/{target_id}/Bulk
[Operations: ALL]

Perform bulk operations on a specified target service provider.

4 Schema

To supported targeted operations, additional schema is defined to support new schema objects namely "targets" and to support extensions to User and Group objects. To support targeted operations, the SCIM schema is extended per section 4 of [draft-scim-core-schema-00].

When extending schema to support targeting, the following URI MUST be added to the "schemas" attribute URI: 'urn:scim:schemas:extension:targeted:1.0'.

4.1 Attributes (multi-valued)

accountRefs A complex multi-valued attribute containing references to associated resources in other targets. Each reference consists of a target identifier and a User object identifier. For each targetId, there may be one or more related object identifiers within each target. An individual identifier can be designated as a primary within a target.

4.2 SCIM Target Schema The Target extension provides a schema for representing the Service Provider's configured target entities

identified using the following URI: 'urn:scim:schemas:extension:targeted:1.0'.

The Target Resource enables a Service Provider to expose the addressable targets reachable within the Service Provider as gatewayed entities. All attributes are READ-ONLY.

5 JSON Representation

5.1 User with Targeted References Representation

The following is a non-normative example of a minimal SCIM representation of a User extended with targeted references in JSON format. The example user has 2 email accounts and one CRM account.

```
{
  "schemas":
    [
      "urn:scim:schemas:core:1.0",
      "urn:scim:schemas:extensions:targeted:1.0:resourceRef"
    ],
  "id": "2819c223-7f76-453a-919d-413861904646",
  "userName": "bjensen@example.com"
  "urn:scim:schemas:extensions:targeted:1.0":{
    "accountRefs":[
```

```
           {
              "targetId":"mail"
              "Display":"Cloud Email Service"
              "references":[
                {
                  "type":"User",
                  "value":"bjensen@example.com",
                  "primary":true
                },
                {
                  "type":"User",
                  "value":"b.jensen@example.com"
                }
              ]
            },
            {
              "targetId":"crm"
              "Display":"Customer Relationship Management Service"
              "references":[
                {
                  "type":"User",
                  "value":"2819c223-7f76-453a-919d-413861904646",
                  "primary":true
                }
              ]
            }
          ]
        }
      }
```

[[Does it make sense to reference Group objects? Others?]]

5.2 Server Config with Targeting Representation The following is a non-normative example of server configuration with targeting schema (indicating the server is a SCIM provisioning "hub") in JSON format.

```
      {
       "schemas": ["urn:scim:schemas:core:1.0",
         "urn:scim:schemas:extensions:targeted:1.0"],
       "documentationUrl":"http://example.com/help/scim.html",
       "patch": {
         "supported":true
       },
       "bulk": {
         "supported":true,
         "maxOperations":1000,
         "maxPayloadSize":1048576
```

```
 },
 "filter": {
   "supported":true,
   "maxResults": 200
 },
 "changePassword" : {
   "supported":true
 },
 "sort": {
   "supported":true
 },
 "etag": {
   "supported":true
 },
 "xmlDataFormat": {
   "supported":true
 },
 "authenticationSchemes": [
   {
     "name": "OAuth Bearer Token",
     "description":
       "Authentication Scheme using the OAuth Bearer Token",
     "specUrl":
       "http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-01",
     "documentationUrl":"http://example.com/help/oauth.html",
     "type":"oauthbearertoken",
     "primary": true
   },
   {
     "name": "HTTP Basic",
     "description": "Authentication Scheme using the Http Basic",
     "specUrl":"http://www.ietf.org/rfc/rfc2617.txt",
     "documentationUrl":"http://example.com/help/httpBasic.html",
     "type":"httpbasic"
    }
 ],
 "urn:scim:schemas:extensions:targeted:1.0": [
   {
     "type":"hub"
   }
 ]
}
```

5.3 Target Representation

The following is a non-normative example of the representation of a Target object in JSON format.

```
      {
        "schemas":["urn:scim:schemas:core:1.0",
          "urn:scim:extensions:targeted:1.0"],
        "id" : "mail",
        "description" : "Corporate imap service",
        "type" : "spoke"
      }
```

5.4 Target Resource Schema Extensions

The following is a normative example of the SCIM Targeted schema extension representation in JSON format.

```
      {
        "id":
          "urn:scim:schemas:extensions:targeted:1.0:resourceRef",
        "name":"Targeted",
        "description":"Targeted Resource Extension",
        "schema":
          [
            "urn:scim:schemas:core:1.0",
            "urn:scim:schemas:extensions:targeted:1.0"
          ],
        "attributes":[
          {
            "name":"accountRefs",
            "type":"complex",
            "multiValued":true,
            "multiValuedAttributeChildName":"targetId",
            "schema":[
              "urn:scim:schemas:core:1.0",
              "urn:scim:schemas:extensions:targeted:1.0"
            ]
            "readOnly":false,
            "required":false,
            "caseExact":true,
            "subAttributes":[
              {
                "name":"targetId",
                "type":"string",
                "multiValued":false,
                "description":"Identifier of target system where
                               one or more related resources can
                               be found",
                "readOnly":false,
                "required":true,
         "caseExact":false
              },
```

```
              {
                "name":"display",
                "type":"string",
                "multiValued":false,
                "description":"A human readable description of
                               target used for display purposes",
                "readOnly":true,
                "required":false,
         "caseExact":false
              },
              {
                "name":"references",
                "type":"complex",
                "multiValued":true,
                "description":"A set of one or more target references
                               for the object within the target.
                "readOnly":false,
                "required":true,
         "caseExact":false
                "subAttributes":[
                  {
                    "name":"type",
                    "type": "string",
                    "multiValued":false,
                    "required":true,
                    "canonicalValues":["User","Group"]
                  },
                  {
                    "name":"value",
                    "type":"string",
                    "multiValued":true,
                    "description":"Unique identifier for the SCIM
                             resource as defined within a target.
                             defined by the Service Provider. Each
                             representation of the resource MUST
                             include a non-empty id value. This
                             identifier MUST be unique across the
                             Target's entire set of resources. It
                             MUST be a stable, non-reassignable
                             identifier that does not change when
                             the same resource is returned in
                             subsequent requests. The value of the id
                             attribute is always issued by the Target
                             Provider and MUST never be specified by
                             the Target Service Consumer. REQUIRED.",
                    "schema":"urn:scim:schemas:core:1.0",
                    "readOnly":true,
                    "required":true,
```

```
                    "caseExact":false
                  },
                  {
                    "name":"primary",
                    "type":"boolean",
                    "multiValued:false,
                    "description":"A Boolean value indicating the
                                  'primary' or default targeted object
                                  for the parent object",
                   "readOnly":false,
                   "required":false,
                   "caseExact":false
                  }

                ]
              }
      [[TBD: what about flags such as isWriteable, etc]]
            ]

          }
        ]
      }
```

6 XML Schema Representation [[TO BE DETERMINED]]

7 Security Considerations

[[TBD]]

No additional security considerations other than those listed in [draft-scim-api-00].

8 IANA Considerations

<IANA considerations text>

9 References

9.1 Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[draft-scim-api-00] Drake, T., "Simple Cloud Identity Management: Protocol 1.0", March 15 2012

[draft-scim-core-schema-00] Mortimore, C., "Simple Cloud Identity Management: Core Schema 1.0", March 15 2012

9.2 Informative References

Appendix A - Editors Notes

The editor would like to thank Gary Cole for his extensive advice and wisdom in advising on how to add Target functions to the SCIM 1.0. The SCIM Target proposal builds in large part on his proposal work in the OASIS RESTpml work, and is shared with his agreement.

Change History

Draft 01 is an administrative update to refresh expiry dates.

Authors' Addresses

Phil Hunt
Oracle Corporation

EMail: phil.hunt@yahoo.com