SCIM
Internet-Draft
Intended status: Standards Track
Expires: 19 April 2026

D. Zollner
Microsoft
U. Vartak
Okta

16 October 2025

SCIM Roles and Entitlements Extension
draft-ietf-scim-roles-entitlements-01

Abstract

The System for Cross-domain Identity Management (SCIM) protocol schema, defined in RFC [RFC7643] defines the complex core schema attributes "roles" and "entitlements". For both of these concepts, frequently only a predetermined set of values are accepted by a SCIM service provider. The values that are accepted may vary per customer or tenant based on customizable configuration in the service provider’s application or based on other criteria such as what services have been purchased or resources associated with entitlements. This document defines an extension to the SCIM 2.0 standard to allow SCIM service providers to represent available data pertaining to SCIM resources, roles and entitlements so that SCIM clients can consume this information and provide easier management of SCIM resources, role and entitlement assignments.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the System for Cross-domain Identity Management Working Group mailing list (scim@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/scim/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-scim-wg/draft-ietf-scim-roles-entitlements.

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 https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Consuming Roles and Entitlements with SCIM Clients . . . 3
2. Conventions and Definitions 3
3. Roles and Entitlements 4
3.1. ServiceProviderConfig Extension 4
3.2. Role Resource Schema 5
3.3. Entitlement Resource Schema 7
3.3.1. Schema samples 9
3.3.2. Sample Roles and Entitlements resource endpoints . . 14
4. References 20
4.1. Normative References 20
4.2. Informative References 20
Appendix A. IANA Considerations 20
Appendix B. Change Log 20
Acknowledgments 21
Authors' Addresses 21

1. Introduction

The System for Cross-domain Identity Management (SCIM) protocol's schema RFC [RFC7643] defines the complex core schema attributes "roles" and "entitlements". For both of these concepts, frequently only a predetermined set of values are accepted by a SCIM service provider. Available roles and entitlements may change based on a variety of factors, such as what features are enabled or what

customizations have been made in a specific instance of a multi-tenant application. Moreover roles and entitlements may be associated with specific SCIM resources within the SCIM server. The core SCIM 2.0 RFC documents ([RFC7642], [RFC7643] and [RFC7644]) do not provide a method for retrieving the available roles or entitlements and the resources associated with roles or entitlements as part of the SCIM 2.0 standard.

In order to allow for SCIM clients to reduce predictable errors when interacting with SCIM service providers, this document aims to provide a method for SCIM service providers to provide data on what roles and/or entitlements are available, the association between roles and/or entitlements and specific resources so that SCIM clients can consume this data to more efficiently manage resources between directories.

1.1. Consuming Roles and Entitlements with SCIM Clients

When a SCIM service provider publishes role and entitlement definitions, SCIM clients can consume them efficiently. The process generally follows these steps:

1. Check Provider Support: Check the ServiceProviderConfig Extension (Section 3.1) for support for roles and entitlements and the resources associated with roles or entitlements.

2. Discover ResourceTypes: Query the /ResourceTypes endpoint to discover which standard and custom role and entitlement resource types (https://datatracker.ietf.org/doc/html/rfc7644#section-4) are supported.

3. Discover schemas for ResourceTypes: Fetch the corresponding schemas (Section 3.3.1) from the /Schemas endpoint, matching them with the ResourceType URNs.

4. Consume resource-specific endpoints (Section 3.3.2) to retrieve the actual supported values for these defined resource types.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Roles and Entitlements

The Roles and Entitlements SCIM Extension consists of two new resource types, /Roles and /Entitlements, as well as accompanying ServiceProviderConfig details to advertise support for this extension. In addition to the new resource types, service providers can use schema extensions to publish custom entitlements.

3.1. ServiceProviderConfig Extension

SCIM endpoints that have implemented one or both of the endpoints from this extension MUST advertise which elements are implemented in the ServiceProviderConfig (https://datatracker.ietf.org/doc/html/rfc7643#section-5) endpoint as defined:

RolesAndEntitlements
: A complex type that specifies Roles and Entitlements extension configuration options. REQUIRED.

roles
: A complex type that specifies configuration options related to the Roles resource type. REQUIRED.

supported
: A boolean type that indicates if the SCIM service provider supports the /Roles endpoint defined in this extension. REQUIRED.

multipleRolesSupported
: A boolean type that indicates if the SCIM service provider supports multiple values for the "roles" attribute on the User resource. OPTIONAL.

primarySupported
: A boolean type that indicates if the SCIM service provider supports the "primary" sub-attribute for the "roles" attribute on the User resource. OPTIONAL.

typeSupported
: A boolean type that indicates if the SCIM service provider supports the "type" sub-attribute for the "roles" attribute on the User resource. OPTIONAL.

types
: A multivalue attribute containing list of types supported for "roles" attribute on the User resource. OPTIONAL.

entitlements
: A complex type that specifies configuration options

related to the Entitlements resource type. REQUIRED.

supported
: A boolean type that indicates if the SCIM service provider supports the /Entitlements endpoint defined in this extension. REQUIRED.

multipleEntitlementsSupported
: A boolean type that indicates if the SCIM service provider supports multiple values for the "entitlements" attribute on the User resource. OPTIONAL.

primarySupported
: A boolean type that indicates if the SCIM service provider supports the "primary" sub-attribute for the "entitlements" attribute on the User resource. OPTIONAL.

typeSupported
: A boolean type that indicates if the SCIM service provider supports the "type" sub-attribute for the "entitlements" attribute on the User resource. OPTIONAL.

types
: A multivalue attribute containing list of types supported for "entitlements" attribute on the User resource. OPTIONAL.

3.2. Role Resource Schema

The /Role resource type has a schema consisting of most of the attributes defined for the User resource’s complex attribute "roles" in [RFC7643], as well as an additional "supported" attribute so that SCIM service providers can indicate if the role is currently enabled and intended for use in their service. The following singular attributes are defined:

id
A unique identifier for the role as defined by the service provider. If present, each representation of the resource MUST include a non-empty "id" value. 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 service provider and MUST NOT be specified by the client. This attribute is OPTIONAL.

value
The value of a role. REQUIRED.

display
A human-readable name, primarily used for display purposes. OPTIONAL.

type
A label indicating the role's function. OPTIONAL
supported
A boolean type that indicates if the role is supported and usable in the SCIM service provider's system. REQUIRED.

limitedAssignmentsPermitted
A boolean type that indicates if a limited number of users may be assigned this role. A value of false should be interpreted as no numerical restriction on the number of users that may hold this role. Other restrictions may exist. OPTIONAL.

totalAssignmentsPermitted
An integer type that indicates how many users may be assigned this role, either directly or inherited. OPTIONAL, but RECOMMENDED if assignments are restricted to a certain number.

totalAssignmentsUsed
An integer type that indicates how many users are currently assigned this role, either directly or inherited. OPTIONAL, but RECOMMENDED if assignments are restricted to a certain number.

Additionally, the following multi-valued attributes are defined:

containedBy
: A list of "parent" roles that contain a superset of permissions including those granted by this role. OPTIONAL.

contains
: A list of "child" roles that this role grants the rights of. OPTIONAL.

3.3. Entitlement Resource Schema

The /Entitlement resource type has a schema consisting of most of the attributes defined for the User resource’s complex attribute "entitlements" in [RFC7643], as well as an additional "supported" attribute so that SCIM service providers can indicate if the entitlement is currently enabled and intended for use in their service.

The following singular attributes are defined:

id
: A unique identifier for the entitlement as defined by the service provider. If present, each representation of the resource MUST include a non-empty "id" value. 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 service provider and MUST NOT be specified by the client. This attribute is OPTIONAL.

value
: The value of an entitlement. REQUIRED.

display
: A human-readable name, primarily used for display purposes. OPTIONAL.

type
: A label indicating the entitlement’s function. OPTIONAL.

supported
: A boolean type that indicates if the entitlement is enabled and usable in the SCIM service provider’s system. OPTIONAL.

limitedAssignmentsPermitted
: A boolean type that indicates if a limited number of users may be assigned this entitlement. A value of false should be interpreted as no numerical restriction on the number of users that may hold this entitlement. Other restrictions may exist. RECOMMENDED.

totalAssignmentsPermitted
: An integer type that indicates how many users may be assigned this entitlement, either directly or inherited. OPTIONAL, but RECOMMENDED if limitedAssignmentsPermitted is true.

totalAssignmentsUsed
: An integer type that indicates how many users are currently assigned this entitlement, either directly or inherited. OPTIONAL, but RECOMMENDED if limitedAssignmentsPermitted is true.

Additionally, the following multi-valued attributes are defined:

containedBy
A list of "parent" entitlements that contain a superset of permissions including those granted by this entitlement. OPTIONAL.

contains
A list of "child" entitlements that this entitlement grants the rights of. OPTIONAL.

3.3.1. Schema samples

3.3.1.1. Role

<base>/scim/v2/Schemas/urn:ietf:params:scim:schemas:core:2.0:Role

Sample schema for a Role property

```
{
 "id":"urn:ietf:params:scim:schemas:core:2.0:Role",
 "name":"Role",
 "description":"Role schema",
 "attributes":[
     {
         "name" : "id",
         "type" : "string",
         "multiValued" : false,
         "description" : "The unique identifier for the role.",
         "required" : false,
         "caseExact" : false,
         "mutability" : "readOnly",
         "returned" : "default",
         "uniqueness" : "none"
     },
     {
         "name" : "value",
         "type" : "string",
         "multiValued" : false,
         "description" : "The value of a role.",
         "required" : true,
         "caseExact" : false,
         "mutability" : "readOnly",
         "returned" : "default",
         "uniqueness" : "none"
     },
     {
         "name" : "display",
         "type" : "string",
         "multiValued" : false,
```

```
            "description" : "A human-readable name, primarily used for display purposes.
 READ-ONLY.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "type",
            "type" : "string",
            "multiValued" : false,
            "description" : "A label indicating the attribute’s function.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "primary",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "A Boolean value indicating the ’primary’ or preferred attrib
ute value for this attribute.  The primary attribute value ’true’ MUST appear no more tha
n once.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "supported",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "supported value for role",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "limitedAssignmentsPermitted",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "if a limited number of users may be assigned this role.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
```

```
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "totalAssignmentsPermitted",
            "type" : "integer",
            "multiValued" : false,
            "description" : "number of users may be assigned this role, either directly o
r inherited.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "totalAssignmentsUsed",
            "type" : "integer",
            "multiValued" : false,
            "description" : "how many users are currently assigned this role, either dire
ctly or inherited.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "containedBy",
            "type" : "string",
            "multiValued" : true,
            "description" : "A list of "parent" roles that contain a superset of permissi
ons including those granted by this role.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "contains",
            "type" : "string",
            "multiValued" : true,
            "description" : "A list of "child" roles that this role grants the rights of.
",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        }
    ]
```

```
}
```

3.3.1.2. Entitlement

<base>/scim/v2/Schemas/
urn:ietf:params:scim:schemas:core:2.0:Entitlement

Sample schema for entitlement property

```
{
    "id":"urn:ietf:params:scim:schemas:core:2.0:Entitlement",
    "name":"Entitlement",
    "description":"Entitlement schema",
    "attributes":[
        {
            "name" : "id",
            "type" : "string",
            "multiValued" : false,
            "description" : "The unique identifier for the Entitlement.",
            "required" : true,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "value",
            "type" : "string",
            "multiValued" : false,
            "description" : "The value of an entitlement.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "display",
            "type" : "string",
            "multiValued" : false,
            "description" : "A human-readable name, primarily used for display purposes.
 READ-ONLY.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
```

```
            "name" : "type",
            "type" : "string",
            "multiValued" : false,
            "description" : "A label indicating the attribute’s function.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "primary",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "A Boolean value indicating the ’primary’ or preferred attrib
ute value for this attribute.  The primary attribute value ’true’ MUST appear no more tha
n once.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "supported",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "supported value for entitlement",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "limitedAssignmentsPermitted",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "if a limited number of users may be assigned this entitlemen
t.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "totalAssignmentsPermitted",
            "type" : "integer",
            "multiValued" : false,
            "description" : "number of users may be assigned this entitlement, either dir
ectly or inherited.",
```

```
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "totalAssignmentsUsed",
            "type" : "integer",
            "multiValued" : false,
            "description" : "how many users are currently assigned this entitlement, eith
er directly or inherited.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "containedBy",
            "type" : "string",
            "multiValued" : true,
            "description" : "A list of "parent" entitlement that contain a superset of pe
rmissions including those granted by this entitlement.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        },
        {
            "name" : "contains",
            "type" : "string",
            "multiValued" : true,
            "description" : "A list of "child" roles that this entitlement grants the rig
hts of.",
            "required" : false,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "none"
        }
    ]
}
```


3.3.2. Sample Roles and Entitlements resource endpoints

3.3.2.1. Retrieving all Roles

```
GET /Roles
```

```
{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":"3",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
            "id":"rl3456",
            "value":"global_lead",
            "display":"Global Team Lead",
            "contains":["us_team_lead"],
            "containedBy":[]
        },
        {
            "id":"rl5873",
            "value":"us_team_lead",
            "display":"U.S. Team Lead",
            "contains":["regional_lead"],
            "containedBy":["global_lead"]
        },
        {
            "id":"rl9057",
            "value":"nw_regional_lead",
            "display":"Northwest Regional Lead",
            "contains":[],
            "containedBy":["us_team_lead"]
        }
    ]
}
```


3.3.2.2. Retrieving all entitlements

```
GET /Entitlements
```

```
{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":"5",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
            "id": "e-10045",  // Internal ID for the Full Access License object
            "value": "license.full_access_seat",
            "type": "License",
            "display": "DevTrack Full Feature License"
            "contains":[],
            "containedBy":[]
        },
        {
            "id": "e-20993",  // Internal ID for the Code Review Bypass permission object
            "value": "feature.code_review_bypass",
            "type": "Permission",
            "display": "Bypass Mandatory Code Review (Elevated Privilege)"
            "contains":[],
            "containedBy":[]
        },
        {
            "id": "e-31578",  // Internal ID for the Storage Limit object
            "value": "storage.limit_100gb",
            "type": "ResourceLimit",
            "display": "100 GB Repository Storage Limit"
            "contains":[],
            "containedBy":["e-10045"]
        }
    ]
}
```

3.3.2.3. Sample user representation with role and entitlement

```
{
    "schemas":
      ["urn:ietf:params:scim:schemas:core:2.0:User",
        "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
        "urn:ietf:params:scim:schemas:core:2.0:Role",
        "urn:ietf:params:scim:schemas:core:2.0:Entitlement"],
    "id": "2819c223-7f76-453a-919d-413861904646",
    "externalId": "701984",
    "userName": "bjensen@example.com",
    "name": {
      "formatted": "Ms. Barbara J Jensen, III",
      "familyName": "Jensen",
      "givenName": "Barbara",
```

```
      "middleName": "Jane",
      "honorificPrefix": "Ms.",
      "honorificSuffix": "III"
    },
    "displayName": "Babs Jensen",
    "nickName": "Babs",
    "profileUrl": "https://login.example.com/bjensen",
    "emails": [
      {
        "value": "bjensen@example.com",
        "type": "work",
        "primary": true
      },
      {
        "value": "babs@jensen.org",
        "type": "home"
      }
    ],
    "addresses": [
      {
        "streetAddress": "100 Universal City Plaza",
        "locality": "Hollywood",
        "region": "CA",
        "postalCode": "91608",
        "country": "USA",
        "formatted": "100 Universal City Plaza\nHollywood, CA 91608 USA",
        "type": "work",
        "primary": true
      },
      {
        "streetAddress": "456 Hollywood Blvd",
        "locality": "Hollywood",
        "region": "CA",
        "postalCode": "91608",
        "country": "USA",
        "formatted": "456 Hollywood Blvd\nHollywood, CA 91608 USA",
        "type": "home"
       }
    ],
    "phoneNumbers": [
      {
        "value": "555-555-5555",
        "type": "work"
      },
      {
        "value": "555-555-4444",
        "type": "mobile"
      }
```

```
    ],
    "ims": [
      {
        "value": "someaimhandle",
        "type": "aim"
      }
    ],
    "photos": [
      {
        "value":
          "https://photos.example.com/profilephoto/72930000000Ccne/F",
        "type": "photo"
      },
      {
        "value":
          "https://photos.example.com/profilephoto/72930000000Ccne/T",
        "type": "thumbnail"
      }
    ],

    "userType": "Employee",
    "title": "Tour Guide",
    "preferredLanguage": "en-US",
    "locale": "en-US",
    "timezone": "America/Los_Angeles",
    "active":true,
    "password": "t1meMa$heen",
    "groups": [
      {
        "value": "e9e30dba-f08f-4109-8486-d5c6a331660a",
        "$ref": "../Groups/e9e30dba-f08f-4109-8486-d5c6a331660a",
        "display": "Tour Guides"
      },
      {
        "value": "fc348aa8-3835-40eb-a20b-c726e15c55b5",
        "$ref": "../Groups/fc348aa8-3835-40eb-a20b-c726e15c55b5",
        "display": "Employees"
      },
      {
        "value": "71ddacd2-a8e7-49b8-a5db-ae50d0a5bfd7",
        "$ref": "../Groups/71ddacd2-a8e7-49b8-a5db-ae50d0a5bfd7",
        "display": "US Employees"
      }
    ],
    "x509Certificates": [
      {
        "value":
         "MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
```

```
          EzARBgNVBAgMCkNhbGlmb3JuaWExFDASBgNVBAoMC2V4YW1wbGUuY29tMRQwEgYD
          VQQDDAtleGFtcGxlLmNvbTAeFw0xMTEwMjIwNjI0MzFaFw0xMjEwMDQwNjI0MzFa
          MH8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQKDAtl
          eGFtcGxlLmNvbTEhMB8GA1UEAwwYTXMuIEJhcmJhcmEgSiBKZW5zZW4gSUlJMSIw
          IAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B
          AQEFAAOCAQ8AMIIBCgKCAQEA7Kr+Dcds/JQ5GwejJFcBIP682X3xpjis56AK02bc
          1FLgzdLI8auoR+cC9/Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5i
          PSi8xO8SL7I7SDhcBVJhqVqr3HgllEG6UClDdHO7nkLuwXq8HcISKkbT5WFTVfFZ
          zidPl8HZ7DhXkZIRtJwBweq4bvm3hM1Os7UQH05ZS6cVDgweKNwdLLrT51ikSQG3
          DYrl+ft781UQRIqxgwqCfXEuDiinPh0kkvIi5jivVu1Z9QiwlYEdRbLJ4zJQBmDr
          SGTMYn4lRc2HgHO4DqB/bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNV
          HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
          Y2F0ZTAdBgNVHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/gwHwYDVR0jBBgwFoAU
          dGeKitcaF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEAA81SsFnOdYJt
          Ng5Tcq+/ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAbOkNngX8+pKfTiDz1R
          C4+dx8oU6Za+4NJXUjlL5CvV6BEYb1+QAEJwitTVvxB/A67g42/vzgAtoRUeDov1
          +GFiBZ+GNF/cAYKcMtGcrs2i97ZkJMo="
      }
    ],
    "entitlements":[
        {
            "id": "e-31578",
            "value": "storage.limit_100gb",
            "type": "ResourceLimit",
            "display": "100 GB Repository Storage Limit",
      }
    ],
    "roles":[
      {
        "value":"global_lead",
        "display":"global lead"
      }
    ],

    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
      "employeeNumber": "701984",
      "costCenter": "4130",
      "organization": "Universal Studios",
      "division": "Theme Park",
      "department": "Tour Operations",
      "manager": {
        "value": "26118915-6090-4610-87e4-49d8ca9f808d",
        "$ref": "../Users/26118915-6090-4610-87e4-49d8ca9f808d",
        "displayName": "John Smith"
      }
    },
    "meta": {
      "resourceType": "User",
```

```
      "created": "2010-01-23T04:56:22Z",
      "lastModified": "2011-05-13T04:42:34Z",
      "version": "W\/\"3694e05e9dff591\"",
      "location": "https://example.com/v2/Users/2819c223-7f76-453a-919d-413861904646"
    }
}
```

~~~

4. References

4.1. 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, <https://www.rfc-editor.org/rfc/rfc2119>.

[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, <https://www.rfc-editor.org/rfc/rfc7643>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

4.2. Informative References

[RFC7642] LI, K., Ed., Hunt, P., Khasnabish, B., Nadalin, A., and Z. Zeltsan, "System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements", RFC 7642, DOI 10.17487/RFC7642, September 2015, <https://www.rfc-editor.org/rfc/rfc7642>.

[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, <https://www.rfc-editor.org/rfc/rfc7644>.

Appendix A. IANA Considerations

(To-Do)

Appendix B. Change Log

-01
~~~

* Added root schema definition for Role and Entitlements properties

* Added id attribute to allow service providers to uniquely identify roles and entitlements

* Defines custom namespace for SPs to define their own schema extensions

* Added examples of requests and responses

* Added Unmesh Vartak as co-author

* Using schema version 2.0 for roles and entitlements schemas: urn:ietf:params:scim:schemas:core:2.0:Role and urn:ietf:params:scim:schemas:core:2.0:Entitlement

-00

* Adopted by SCIM WG

Acknowledgments

TODO acknowledge.

Authors' Addresses

Danny Zollner
Microsoft
Email: danny@zollnerd.com

Unmesh Vartak
Okta
Email: uvartak@okta.com