Workgroup: SCIM
Internet-Draft:
draft-zollner-scim-roles-entitlements-extension-00
Published: 22 October 2021
Intended Status: Informational
Expires: 25 April 2022
Authors: D. Zollner
Microsoft

SCIM Roles and Entitlements Extension

Abstract

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. 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. This document defines an extension to the SCIM 2.0 standard to allow SCIM service providers to represent available data pertaining to roles and entitlements so that SCIM clients can consume this information and provide easier management of role and entitlement assignments.

Status of This Memo

Copyright Notice

Table of Contents

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. The core SCIM 2.0 RFC documents (RFC7642, RFC7643 and RFC 7644) do not provide a method for retrieving the available roles or entitlements as part of the SCIM 2.0 standard.

In order to allow for SCIM clients to avoid easily 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 so that SCIM clients can consume this data to more efficiently manage resources between directories.

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. IANA Considerations

This document has no IANA actions.

4. 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.

4.1. 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 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.

enabled

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. REQUIRED.

primarySupported

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

typeSupported

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

entitlements

A complex type that specifies configuration options related to the Entitlements resource type. REQUIRED.

enabled

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. REQUIRED.

primarySupported

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

typeSupported

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

4.2. Roles Resource Schema

The /Roles 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 "Enabled" 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:

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

enabled
    A boolean type that indicates if the role is enabled and usable in the SCIM service provider's system. REQUIRED.

4.3. Entitlements Resource Schema

The /Entitlements 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 "Enabled" 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:

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.

enabled
    A boolean type that indicates if the entitlement is enabled and usable in the SCIM service provider's system. REQUIRED.

4.4. Sample Requests

4.4.1. Retrieving all roles

4.4.1.1. Request

```
GET /Roles
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

4.4.1.2. Response

```
HTTP/1.1 200 OK
Content-Type: application/scim+json

{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":3",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
            "value":"admin"
            "display":"Administrator"
            "enabled":True
        },
        {
            "value":"user"
            "display":"User"
            "enabled":True
        },
        {
            "value":"teamlead"
            "display":"Team Leader"
            "enabled":True
        }
    ]
}
```

4.4.2. Retrieving all entitlements

4.4.2.1. Request

```
GET /Entitlements
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

4.4.2.2. Response

```
HTTP/1.1 200 OK
Content-Type: application/scim+json

{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":4",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
            "value":"1"
            "display":"Printing"
            "enabled":True
        },
        {
            "value":"2"
            "display":"Scanning"
            "enabled":True
        },
        {
            "value":"3"
            "display":"Copying"
            "enabled":True
        },
        {
            "value":"4"
            "display":"Collating"
        }
    ]
}
```

5. Roles Schema BNF

```
[
    {
        "id" : "urn:ietf:params:scim:schemas:2.0:Roles",
        "name" : "Role",
        "description" : "Roles available for use with the User
        resource's 'roles' attribute",
        "attributes" : [
            {
                "name" : "value",
                "type" : "string",
                "multiValued" : false,
                "description" : "The value of a role",
                "required" : true,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "display",
                "type" : "string",
                "multiValued" : false,
                "description" : "A human-readable name, primarily
                used for display purposes.",
                "required" : false,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "type",
                "type" : "string",
                "multiValued" : false,
                "description" : "A label indicating the role's
                function.",
                "required" : false,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "enabled",
                "type" : "boolean",
                "multiValued" : false,
                "description" : "A boolean type that indicates if the
                role is enabled and usable in the SCIM service
                provider's system.",
                "required" : true,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default"
            }
        ]
    }
]
```

6. Entitlements Schema BNF

```
[
    {
        "id" : "urn:ietf:params:scim:schemas:2.0:Entitlements",
        "name" : "Entitlement",
        "description" : "Entitlements available for use with the User
        resource's 'entitlements' attribute",
        "attributes" : [
            {
                "name" : "value",
                "type" : "string",
                "multiValued" : false,
                "description" : "The value of an entitlement",
                "required" : true,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "display",
                "type" : "string",
                "multiValued" : false,
                "description" : "A human-readable name, primarily
                used for display purposes.",
                "required" : false,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "type",
                "type" : "string",
                "multiValued" : false,
                "description" : "A label indicating the role's
                function.",
                "required" : false,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default",
                "uniqueness" : "server"
            },
            {
                "name" : "enabled",
                "type" : "boolean",
                "multiValued" : false,
                "description" : "A boolean type that indicates if the
                role is enabled and usable in the SCIM service
                provider's system.",
                "required" : true,
                "caseExact" : false,
                "mutability" : "readOnly",
                "returned" : "default"
            }
        ]
    }
]
```

7. 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/info/rfc2119>.

[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/info/rfc8174>.

Acknowledgments

TODO acknowledge.

Author's Address

Danny Zollner
Microsoft

Email: danny@zollnerd.com