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

SCIM Verified Domains Extension

Abstract

The System for Cross-domain Identity Management (SCIM) protocol supports creation and management of identity resources such as users between a client and a service provider. In some instances, a SCIM service provider may maintain a list of DNS domains that an organization using that service has registered for their exclusive use with the service. This registration of domains is frequently tied to some form of ownership verification for each domain. This document defines an extension to the SCIM protocol introducing a new 'VerifiedDomains' resource type in order to allow a SCIM client to confirm what domains have had ownership verified by the SCIM service provider, as well as some information about whether the User resource's userName and emails attributes require domain verification in order for a value to possess that domain suffix.

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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 April 2022.

Table of Contents

1. Introduction

The System for Cross-domain identity Management (SCIM) protocol RFC7644 supports creation, modification, and deletion of core identity resources. To allow for efficient interactions between SCIM clients and multi-customer SCIM service providers such as SaaS applications, the client may wish to avoid sending creation or update requests that are already known to contain attribute values that will be rejected by the SCIM service provider.

A common source of creation and update failures when interacting with SCIM service providers for SaaS applications is when the SCIM client attempts to create or update the userName(adhering to RFC5321 format) or emails attribute on a user and the SCIM client provides a value with a domain suffix that is not verified in the customer's tenant in the service represented by the SCIM service provider.

This document defines a simple extension to the SCIM protocol and core schema that adds support for a "VerifiedDomains" resource type that can be queried to retrieve a list of verified domains in the SCIM service provider's environment so that a SCIM client can

utilize this information to apply additional logic and avoid sending requests that will fail.

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. Definitions

Domain: At least a Second Level Domain (SLD) and a Top Level Domain(TLD) registered with public DNS registrars and ICANN. Further expansion to Third Level Domains (aka subdomains) are also permitted.

5. Verified Domains

A SCIM endpoint supporting the Domains extension **MUST** implement a /VerifiedDomains resource as outlined in this document. This extension is written with only the HTTP/REST GET method required, as the data provided by the SCIM service provider is intended to be read-only. POST, PUT, PATCH and DELETE requests to the /VerifiedDomains resource **MUST** result in a HTTP Bad Request (400).

5.1. ServiceProviderConfig Extension

SCIM endpoints that support the Verified Domains extension **MUST** advertise this support in the ServiceProviderConfig endpoint as defined:

verifiedDomains
: A complex type that specifies Verified Domains configuration options. REQUIRED.

  supported
  : A boolean type that specifies if the Verified Domains extension is supported.

  userNameProperties
  : A complex type that specifies if the expected value for userName follows the RFC5321 format, and if accepted values following RFC5321 require a verified domain suffix.

  emailsVerifiedDomainRequired
  : A boolean type that specifies if accepted values for emails require a verified domain suffix.

5.2. VerifiedDomains Schema Extension

Any SCIM service provider that supports the Verified Domains extension **MUST** implement the VerifiedDomains resource type with the urn:ietf:params:scim:schemas:2.0:VerifiedDomain schema defined in this section:

The following singular attributes are defined:

domainName
: A string attribute containing at least the Second Level Domain (SLD) and Top Level Domain (TLD) of a domain verified in the SCIM service provider's system. Subdomains (Third Level Domains and below) are supported as well. REQUIRED.

allowSubdomains
: A boolean attribute set to true for any verified domain resource that should be interpreted by the client to include all subdomains. REQUIRED.

verifiedDate
: A dateTime attribute indicating the date and time at which the domain resource was verified in the SCIM service provider's system. OPTIONAL.

5.3. Sample Requests

5.3.1. Retrieving all verified domains

5.3.1.1. Request

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

5.3.1.2. Response

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

{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":2",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
        "id":"1",
        "domainName":"contoso.com",
        "allowSubdomains":true,
        },
        {
        "id":"2",
        "domainName":"fabrikam.com",
        "allowSubdomains":true
        }
    ]
}
```

5.3.2. Querying verified domains by domainName value

5.3.2.1. Request

```
GET /VerifiedDomains?filter=domainName contains "contoso.com"
Host: example.com
Accept: application/scim+json
Authorization: Bearer 123456abcd
```

5.3.2.2. Response

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

{
    "schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],
    "totalResults":1",
    "itemsPerPage":100,
    "startIndex":1,
    "Resources":[
        {
        "id":"1",
        "domainName":"contoso.com",
        "allowSubdomains":true
        }
    ]
}
```

6. Schema BNF

```
[
    {
        "id" : "urn:ietf:params:scim:schemas:2.0:VerifiedDomain",
        "name" : "Domain",
        "description" : "DNS Domains",
        "attributes" : [
            {
            "name" : "domainName"
            "type" : "string"
            "multiValued" : false
            "description" : "Value for a domain name registered and
            optionally verified in the SCIM service provider. The
            value should represent a DNS domain name such as
            'contoso.com' and optionally may contain
            one or more subdomain levels such as 'scim.contoso.com'.
            REQUIRED.",
            "required" : true,
            "caseExact" : false,
            "mutability" : "readOnly",
            "returned" : "default",
            "uniqueness" : "server"
            },
            {
            "name" : "allowSubdomains",
            "type" : "boolean",
            "multiValued" : false,
            "description" : "A Boolean value indicating if subdomains
            below the domain specified in domainName should be
            treated identically to the value provided in domainName.
            OPTIONAL",
            "required" : true,
            "mutability" : "readOnly",
            "returned" : "default"
            },
            {
            "name" : "verifiedDate",
            "type" : "dateTime",
            "multiValued" : false,
            "description" : "An optional dateTime value indicating
            the time at which the domain specified in domainName
            was verified. OPTIONAL",
            "required" : false
            "mutability" : "readOnly",
            "returned" : "default"
            }
        ]
        "meta" : {
        "resourceType" : "Schema",
        "location" :
```

```
        "/v2/Schemas/urn:ietf:params:scim:schemas:2.0:VerifiedDomain"
        }
    }
]
```

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