SCIM Extension Drafts: Domains, Roles + Entitlements

Danny Zollner

IETF 112

November 11, 2021

Verified Domains

- Draft written to address SaaS problem requiring domains to be ownership verified prior to usage
  - Mail providers, collaboration platforms, etc. frequently require proof of domain ownership
- Username* and emails.value frequently require domain suffix to have ownership verified in SaaS system
  - * If userName is required to be in user@domain.com format
- Requests fail if domain suffix on userName or emails.value is not verified in SaaS system
- Implements new resource endpoint for SCIM client to list available domains and consider that in logic while deciding if it should send a request
- Draft located: https://datatracker.ietf.org/doc/draft-zollner-scim-domain-extension/

Verified Domains – Key Components

- Adds /VerifiedDomains resource
  - Read only – only HTTP GET supported
  - Some SCIM service providers have interest in trusting domain verification from connected IdPs, but security concerns on how to establish trust and avoid bad actors impersonating an IdP led to decision to simplify to only GET
- Adds verifiedDomains ServiceProviderConfig extension

Verified Domains - Schema

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.

Verified Domains - ServiceProviderConfig

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
- 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.

Verified Domains – Open Questions

- Is RFC5321 the correct RFC to point to for user@domain.com format?
  - It is called out as the standard for email.value in SCIM RFC 7643

- AllowSubdomains – added for instances where different tenants/environments in SCIM service provider may have different subdomains. i.e. eu.example.com exists in a separate SCIM-connected directory than example.com, meaning ownership of example.com should not extend to all subdomains
  - Is the purpose of this clear?
  - Should this be moved to optional and guidance added specifying that if the value is not provided it is assumed to be true?

- General feedback needed on descriptive sections of draft defining domains, verified domains concept, etc.

Roles + Entitlements

- Draft written to solve challenges faced by SCIM clients when dealing with roles and entitlements
  - Discovery of acceptable values for user resource's roles and entitlements attributes in order to prevent invalid/rejected requests
  - Discovery of available roles and entitlements values for user resource for the purpose of mapping/assignment in SCIM client
- Draft located: https://datatracker.ietf.org/doc/draft-zollner-scim-roles-entitlements-extension/

Roles + Entitlements – Key Components

- Adds /Roles resource
- Adds /Entitlements resource
- Adds ServiceProviderConfig extension

Roles + Entitlements - Schema

- Mostly mimics sub-attributes of user resource attributes
  - value
  - display
  - type
- Adds one new attribute
  - enabled

Roles + Entitlements - ServiceProviderConfig

roles *(duplicated for entitlements)*

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.

Roles + Entitlements - Open Questions

- How widely adopted is the type sub-attribute for roles and entitlements?
  - Should this be included as a role/entitlement-specific attribute?
    - Is type a universal concept rather than role/entitlement-specific? Should valid values for type be communicated somewhere else – e.g.: ServiceProviderConfig?
  - Should it remain as a sub-attribute in the core schema doc?
  - Should type sub-attribute be removed from user resource's roles attribute?
- Should this be a standalone extension or merged into the core schema docs?