Technische Referenz

System for Cross-Domain Identity Management im Kontext Provisionierung

Februar 2024

Inhaltsverzeichnis

Vorwort....2
Leserkreis....2
Bezugsdokumente....2
Typografische Konventionen....2
Symbol Konventionen....2
Einführung....4
Funktionsweise....4
Begrifflichkeit....4
Modell....5
Repräsentation eines Benutzers....6
Repräsentation einer Gruppe....6
Schema....7
Attributdefinition....7
Datentypen....8
Operationen....9
Ressource suche (Search)....9
Ressource abrufen (WellKnown)....9
Ressource erzeugen (Create)....10
Ressource ersetzen (Replace)....10
Ressource ändern (Update)....11
Resource Löschen (Delete)....11
Erweiterung....12
Datenmodell....12
Schema....12
Endpunkte....12
Operationen....13
Benutzer....13
Gruppen....13
Tenants....13
Berechtigung im Tenant zuweisen....14
Berechtigung im Tenant entziehen....14

Vorwort

Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Administration von Ressourcen, sowie Teams, die sich mit der Integration von Zielsystemen, in Oracle Identity Governance befassen.

Bezugsdokumente

SCIM 2.0 wurde im September 2015 als RFC7642, RFC7643 und RFC7644 durch IETF veröffentlicht.

- RFC7642 - SCIM: Definitions, Overview, Concepts, and Requirements
  In diesem Dokument werden die Szenarien und Anwendungsfälle des Systems für Cross-Domain Identity Management (SCIM) aufgeführt.
- RFC7643 - SCIM: Core Schema
  Das Core Schema definiert ein plattformneutrales Schema und und Modell zur Erweiterung für die Darstellung von Benutzern und Gruppen.
- RFC7644 - SCIM: Protocol
  Das SCIM-Protokoll ist ein REST-Protokoll auf Anwendungsebene zur Bereitstellung und Verwaltung von Identitätsdaten.

Typografische Konventionen

Die folgenden typografischen Konventionen werden in diesem Dokument verwendet:

Konvention	Bedeutung
Fettdruck	Fettdruck kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind.
Kursiv	Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhalter, für die Sie bestimmte Werte angeben.
`Monospace`	Monospace in einem Absatz kennzeichnet Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Konvention	Bedeutung
[ ]	Enthält optionale Argumente und Befehlsoptionen.

Konvention	Bedeutung
{ | }	Enthält eine Reihe von Auswahlmöglichkeiten für eine erforderliche Befehlsoption.
${ }	Referenziert eine Variable.
-	Verbindet gleichzeitig mehrere Tastenanschläge.
+	Verbindet mehrere aufeinanderfolgende Tastenanschläge.
>	Zeigt die Auswahl eines Menüpunkts in der grafischen Benutzeroberfläche an.

Einführung

Die System for Cross-Domain Identity Management (SCIM)-Spezifikation (ursprünglich Simple Cloud Identity Management) soll die Verwaltung von Benutzeridentitäten in Anwendungen und Diensten erleichtern. Die Spezifikation zielt darauf ab, mit definierten Schemata die Bereitstellungen von Benutzerkonten aufzubauen. Dabei wurde besonderer Wert auf die Einfachheit der Entwicklung und Integration gelegt wird und gleichzeitig bestehende Modelle zur Authentifizierung, Autorisierung und dem Datenschutz angewendet. Ziel ist es, die Kosten und Komplexität von Vorgängen der Benutzerverwaltung durch die Bereitstellung eines allgemeinen Benutzerschemas und entsprechenden Erweiterung sowie durch die Bindung von Dokumenten zu reduzieren, um Muster für den Austausch dieses Schemas mithilfe von Standardprotokollen bereitzustellen.

Funktionsweise

SCIM ist ein Protokoll auf der Grundlage von REST und JSON, das eine Client- und eine Server-Rolle definiert. Der Client ist in der Regel ein Identity Provider (IdP) wie Oracle Identity Governance mit einer Datenbank von Benutzeridentitäten. Der Service Provider (SP) ist in der Regel eine Applikation wie Box oder Slack, die eine Teilmenge an Informationen von diesen Identitäten benötigt. Wenn beim IdP Änderungen wie das Erstellen, Aktualisieren und Löschen von Identitäten vorgenommen werden, werden sie automatisch über das SCIM-Protokoll mit dem SP synchronisiert. Der IdP kann auch Identitäten vom SP übernehmen, um seinen Datenbestand zu ergänzen und falsche Werte auf SP-Seite zu erkennen, die zu Sicherheitslücken führen könnten. Für den Endanwender bedeutet dies, dass er nahtlosen Zugriff auf die Anwendungen hat, die ihm zugewiesen sind, wobei diese über aktuelle Profile und Berechtigungen verfügen.

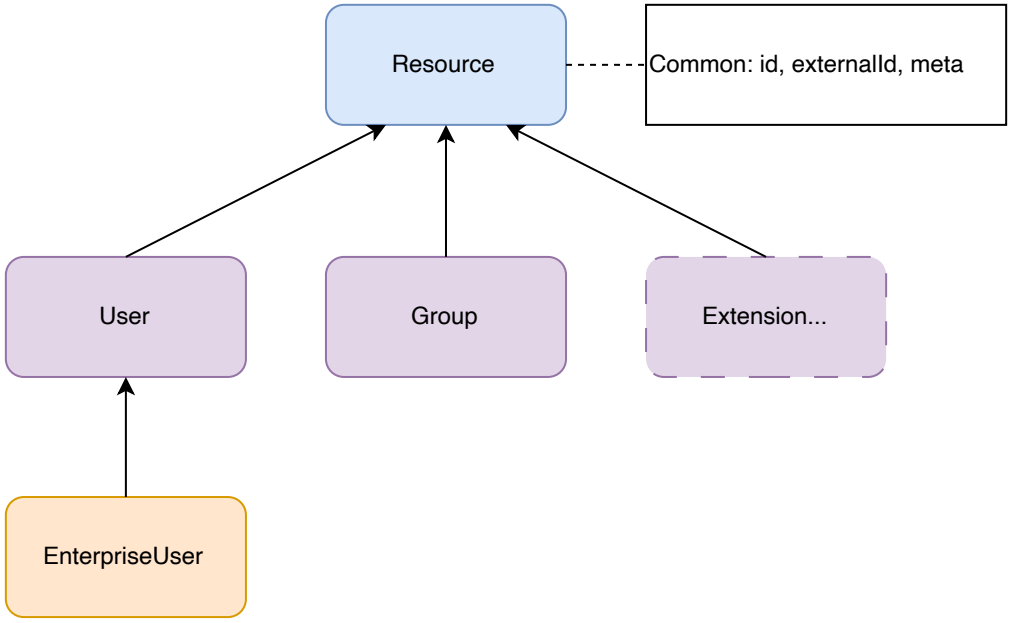
Begrifflichkeit

- Service Provider
  Eine REST-fähige Anwendung, die Informationen zu Identitäten via SCIM Protokoll zur Verfügung stellt.
- Client
  Eine Anwendung, die über SCIM Identitätsdaten verwaltet, die ein Service Provider vorhält (schickt diesem SCIM HTTP Anfragen).
- Ressource
  SCIM 2.0 basiert auf einem Objektmodell. Als gemeinsamer Nenner gilt die Ressource, von der alle anderen Objekte abgeleitet werden.
- Resource Type
  Die Art der Ressource.
  Spezifiziert den Namen von Ressourcen, Endpunkten, URL, Schemas, und andere
- Schema
  Sammlung von Attributdefinitionen, die den Inhalt von Ressourcen beschreiben, z.B. "urn:ietf:params:scim:schemas:core:2.0:User"

Modell

SCIM 2.0 basiert auf einem Objektmodell. Als gemeinsamer Nenner gilt die Ressource, von der alle anderen Objekte abgeleitet werden.

- Resource ist ein JSON Object
- Es besteht aus einem oder mehreren Attributen.
- Diese Attribute können zu einem oder mehreren Schemas gehören



Entsprechend der Vererbung ist **User** in SCIM eine **Resource**.

Jedes Benutzerprofil in einem System verfügt über einen Namen, eine Adresse, Telefonnummern, E-Mail-Adressen usw. Diese gemeinsamen Attribute gelten für jedes Benutzerprofil, das von einem beliebigen System verwaltet wird. Eine Sammlung solcher allgemeiner Benutzerattribute wird als Benutzerressource bezeichnet. Es kann jedoch Situationen geben, in denen die Verwaltung system-/anwendungsspezifischer Attribute für Benutzer erforderlich ist (z. B. Benutzer, die Geräte für die Anwendung anmelden). Aufgrund dieser Tatsache führt SCIM den **EnterpriseUser** als Erweiterung für die Benutzerressource ein. **EnterpriseUser** ist eine Erweiterung des User-Attributs, das eine Sammlung anwendungsspezifischer Attribute enthält.

Darüber hinaus sind „id“, „externalId“ und „meta“ drei allgemeine Attribute, die in jeder SCIM-Ressource enthalten sind, mit Ausnahme der Ressourcen wie „ServiceProviderConfig“ und „ResourceType“, die zur Ermittlung von SCIM-Dienstanbietern und anderen mit der Erkennung der speziellen Eigenschaften von Dienstanbietern verbundenen Ressourcen verwendet werden.

- id
  Eine eindeutige Kennung für eine SCIM-Ressource, die vom SCIM-Dienstanbieter definiert wird. Es wird vom SCIM-Dienstanbieter beim Erstellen der Ressource generiert. Es handelt sich um ein **ERFORDERLICHES** Attribut.
- externalId
  Eine Zeichenfolge, die eine Kennung für die Ressource darstellt, die vom SCIM-Client

generiert wird. Mit anderen Worten: Kennung der ursprünglichen Quelle, aus der die Benutzerdaten stammen (z. B. Datenbank-ID, aus der der Benutzer vom SCIM-Client entnommen wird). Es handelt sich um ein **OPTIONAL**-Attribut.

- meta
  Allgemeine Metadaten für eine Ressource. Sie werden vom SCIM-Dienstanbieter beim Erstellen der Ressource generiert.
  Zum Beispiel: Zeitstempel der Erstellung, Zeitstempel der letzten Änderung, Standort der Ressource. Es handelt sich um ein **ERFORDERLICHES** Attribut.

Repräsentation eines Benutzers

Dies ist ein Beispiel dafür, wie Benutzerdaten als SCIM-Objekt in JSON codiert werden können.

```
{ "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ]
, "id"          : "2819c223-7f76-453a-919d-413861904646"
, "externalId" : "azitterbacke"
, "meta":{
    "resourceType" : "User",
    "created"      : "2011-08-01T18:29:49.793Z",
    "lastModified" : "2011-08-01T18:29:49.793Z",
    "location"     : "https://service-provider/v2/Users/2819c223...",
    "version"      : "W\/\"f250dd84f0671c3\""
  }
, "name": {
    "formatted"       : "Mr. Alfons Zitterbacke, III"
  , "familyName"      : "Zitterbacke"
  , "givenName"       : "Alfons"
  , "honorificPrefix" : "Mr."
  , "honorificSuffix" : "III"
  }
, "userName":"azitterbacke",
, "phoneNumbers" : [
    { "primary" : "true"
    , "type"    : "work"
    , "value"   : "555-555-8377"
    }
  ],
  "emails":[
    { "primary" : true
    , "type"    : "work"
    , "value"   : "azitterbacke@somewhere.com"
    }
  ]
```

Repräsentation einer Gruppe

Zusätzlich zu den Benutzern umfasst SCIM auch die Definitionen von Gruppen. Gruppen werden verwendet, um die Organisationsstruktur bereitgestellter Ressourcen zu modellieren. Gruppen können Benutzer oder andere Gruppen enthalten.

```
{ "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group"
  ]
, "id"          : "e9e30dba-f08f-4109-8486-d5c6a331660a"
, "displayName" : "Clerk"
, "members" : [
    { "value"   : "2819c223-7f76-453a-919d-413861904646"
    , "$ref"    : "https://service-provider/v2/Users/2819c223..."
    , "display" : "Dwight Schrute"
    }
  , { "value"   : "902c246b-6245-4190-8e05-00816be7344a"
    , "$ref"    : "https://service-provider/v2/Users/902c246b..."
    , "display" : "Agathe Musterfrau"
    }
  ],
  "meta": {
    "resourceType" : "Group",
    "created"      : "2010-01-23T04:56:22Z",
    "lastModified" : "2011-05-13T04:42:34Z",
    "version"      : "W\/\"3694e05e9dff592\"",
    "location"     : ""https://service-provider/v2/Groups/e9e30dba..."
  }
}
```

Schema

Schema ist eine Sammlung von Attributdefinitionen, die den Inhalt einer gesamten oder eines Teils der Ressource beschreiben.

Jede Darstellung von Daten ist über JSON definiert.

Attributdefinition

Attributdefinition bedeutet, wie Attribute definiert werden. SCIM-Attributdefinitionen enthalten die folgenden Details:

Type	Bedeutung
Singular Attribute	Attribute einer Ressource, das 0..1 Werte enthalten kann, z.B. „displayName“.
Multi-valued Attribute	Attribute einer Ressource, das 0..n Werte enthalten kann, z.B.: „emails“.
Simple Attribute	Attribute einer Ressource (singular oder multi-valued), dessen Werte einen einfachen Datentyp wie z.B. „String“ hat.
Complex Attribute	Attribute einer Ressource (singular oder multi-valued), dessen Werte aus einer Sammlung von einem oder mehrere Simple Attributes besteht, z.B.: „adresses“.
Sub-Attribute	Ein Simple Attribute, das in einem Complex Attribute enthalten ist.

Beispiel:

```
{ "name"         : "userName"
, "type"         : "string"
, "multiValued" : false
, "description" : "Unique identifier for the User, typically used by ..."
, "required"     : true
, "caseExact"    : false
, "mutability"   : "readWrite"
, "returned"     : "default"
, "uniqueness"   : "server"
}
```

Datentypen

Es gibt eine festgelegte Anzahl von Datentypen. SCIM-Erweiterungen sollen keine neue Datentypen definieren.

Es werden konform zu RFC4627 werden folgende Datentypen spezifiziert:

Type	Bedeutung
String	0..n Unicode Zeichen.
Boolean	Literale „true“ oder „false“
Decimal	Reale Zahl mit mindestens einer Stelle hinter dem Dezimalpunkt, z.B. „3.4“ [=3,4]
Integer	Dezimalzahl ohne gebrochenen Anteil.
DateTime	Datum/Zeit-Angabe im Format: 2008-01-23T04:56:22Z
Binary	Beliebige Binäre Daten, base64-kodiert
Reference (auch $ref)	Eine Referenz zu einer SCIM-Ressource als absolute oder relative URI, z.B.:
Complex	Attribute einer Ressource (singular oder multi-valued), dessen Werte aus einer Sammlung von einem oder mehrere Simple Attributes besteht.

Wenn nicht anders spezifiziert gelten folgende Standards für Attribut-Datentypen:

- optional ("required=false")
- case insensitive ("caseExact=false")
- veränderbar ("mutability=readWrite")
- werden bei Anfragen zurückgegeben ("returned=default")
- sind nicht eindeutig ("uniqueness=none")
- sind vom Datentyp String

Operationen

Für die Manipulation von Ressourcen stellt SCIM eine REST-API mit einer umfangreichen, aber einfachen Reihe von Operationen bereit, die alles vom Patchen eines bestimmten Attributs für einen bestimmten Benutzer bis hin zur Durchführung umfangreicher Massenaktualisierungen unterstützen:

Operation	Methode	Beispiel
Search	GET	https://{service-provider}/{v}/{resource}?filter={attribute}{op}{value}&sortBy={attributeName}&sortOrder={ascending|descending}
WellKnown	GET	https://{service-provider}/{v}/{resource}/{id}
Create	POST	https://{service-provider}/{v}/{resource}
Replace	PUT	https://{service-provider}/{v}/{resource}/{id}
Update	PATCH	https://{service-provider}/{v}/{resource}/{id}
Delete	DELETE	https://{service-provider}/{v}/{resource}/{id}

Ressource suche (Search)

```
GET /Users??startIndex=1&count=10
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
```

Ressource abrufen (WellKnown)

```
GET /Users/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
```

Ressource erzeugen (Create)

```
POST: /Users
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
Content-Length: ...
{ "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ]
, "userName"   : "azitterbacke"
, "externalId" : "azitterbacke"
, "name"       : {
    "formatted"  : "Mr. Alfons Zitterbacke, III"
  , "familyName" : "Zitterbacke"
  , "givenName"  : "Alfons"
  , "honorificPrefix" : "Mr."
  , "honorificSuffix" : "III"
  }
, "emails":[
    { "primary" : true
    , "type"    : "work"
    , "value"   : "alfons.zitterbacke@somewhere.com"
    }
  ]
, "phoneNumbers":[
    { "primary" : true
    , "type"    : "work"
    , "value"   : "55-555-8377"
    }
  ]
}
```

Ressource ersetzen (Replace)

```
PUT /Users/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
Content-Length: ...
{ "id" : {id}
, "name"       : {
    "givenName" : "Alfons"
  }
, "emails":[
    { "primary" : true
    , "type"    : "work"
    , "value"   : "alfons.zitterbacke@nowhere.com"
    }
  ]
}
```

Ressource ändern (Update)

```
PATCH /Users/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
{ "schemas"    : ["urn:ietf:params:scim:api:messages:2.0:PatchOp"]
, "Operations" : [
    { "op"     : "replace"
    , "path"   : "name.givenName"
    , "value"  : "Alfons"
    }
  , { "op"     : "replace"
    , "path"   : "emails[type eq \"work\"].value"
    , "value"  : "alfons.zitterbacke@somewhere.com"
    }
  ]
}
```

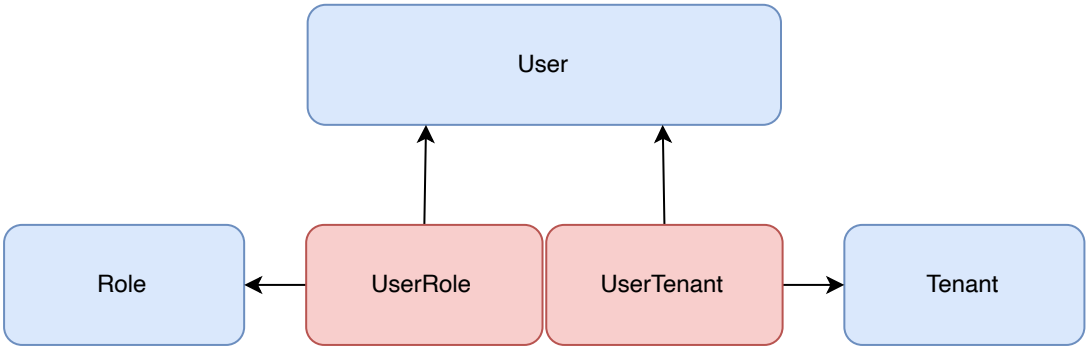
Resource Löschen (Delete)

```
DELETE https://{service-provider}/{context-uri}/Users/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8…
```

Erweiterung

Datenmodell

Folgendes theoretisches Datenmodel, soll durch entsprechende Erweiterung des SCIM-Core Schemas einem hypothetischen Prozess zu Bereitstellung von Benutzerkonten und den damit verbundenen Zuweisungen und Entzug von Berechtigungsobjekten zugrunde gelegt werden.



Schema

Um die Entität „Tenant“ innerhalb der Prozesse der Benutzerverwaltung wird eine Schemaerweiterung deklariert.

Somit exponiert der Service Provider folgende Beziehung zwischen dem Datenmodell und dem erforderlichen SCHIM-Schema:

Entität	Schema
Users	urn:ietf:params:scim:schemas:core:2.0:User
Role	urn:ietf:params:scim:schemas:core:2.0:Group
Tenant	urn:ietf:params:scim:schemas:extension:p20:1.0:Tenant

Endpunkte

Folgende Endpunkte sind hierfür zu implementieren:

Endpunkt	Bedeutung
/Users	Exponiert die Standard-Operationen zur Suche und dem Anlegen, Ändern und Löschen von Benutzerkonten.
/Groups	Exponiert die Standard-Operationen zur Suche und der Zuweisung bzw. dem Entzug von Berechtigungsobjekten in Relation zu Benutzerkonten.
/Tenants	Exponiert die erweiterten Operationen zur Suche und der Zuweisung bzw. dem Entzug von Berechtigungsobjekten in Relation zu Benutzerkonten.

Operationen

Benutzer

- Das im Modell spezifizierte Entität „User“ entspricht dem im RFC7643 definiertem Schema-Objekt „User“.
- Die Operationen zur Suche von Benutzerkonten entsprechen den Standards gemäß RFC7644 - SCIM: Protocol Abschnitt 3.4.
- Die Operationen zum Anlegen, Ändern und Löschen von Benutzerkonten werden gemäß den Standards RFC7644 - SCIM: Protocol Abschnitt 3.3, RFC7644 - SCIM: Protocol Abschnitt 3.5.1 und RFC7644 - SCIM: Protocol Abschnitt 3.6 durch den entsprechenden Endpunkt exponiert.

Gruppen

- Das im Modell spezifizierte Entität „Role“ entspricht dem im RFC7643 definiertem Schema-Objekt „Group“.
- Die Operationen zur Suche diese Berechtigungsobjekts entsprechen den Standards gemäß RFC7644 - SCIM: Protocol Abschnitt 3.4.
- Die Operationen zum Anlegen und Löschen diese Berechtigungsobjekts gemäß den Standards RFC7644 - SCIM: Protocol Abschnitt 3.3, RFC7644 - SCIM: Protocol Abschnitt 3.5.1 und RFC7644 - SCIM: Protocol Abschnitt 3.6 werden NICHT durch den entsprechenden Endpunkt exponiert.
- Die Operation Ändern diese Berechtigungsobjekts beschränkt sich auf die Zuweisung und den Entzug diese Berechtigungsobjekts in Relation zu Benutzerkonten und werden gemäß Standard RFC7644 - SCIM: Protocol Abschnitt 3.5.2 exponiert.
- Die Zuweisung und der Entzug diese Berechtigungsobjekts erfolg über den Endpunkt „/Groups“.

Tenants

- Das im Modell spezifizierte Entität „Tenant“ wird konform zu RFC7643 als Schemaerweiterung „Tenant“.exponiert.
- Die Operationen zur Suche diese Berechtigungsobjekts entsprechen den Standards gemäß RFC7644 - SCIM: Protocol Abschnitt 3.4.
- Die Operationen zum Anlegen und Löschen diese Berechtigungsobjekts gemäß den Standards RFC7644 - SCIM: Protocol Abschnitt 3.3, RFC7644 - SCIM: Protocol Abschnitt 3.5.1 und RFC7644 - SCIM: Protocol Abschnitt 3.6 werden NICHT durch den entsprechenden Endpunkt exponiert.
- Die Operation Ändern diese Berechtigungsobjekts beschränkt sich auf die Zuweisung und den Entzug diese Berechtigungsobjekts in Relation zu Benutzerkonten und werden gemäß Standard RFC7644 - SCIM: Protocol Abschnitt 3.5.2 exponiert.
- Die Zuweisung und der Entzug diese Berechtigungsobjekts erfolg über den Endpunkt „/Tenants“.

Berechtigung zuweisen

```
PPATCH /Tenants/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
{ "schemas"     : ["urn:ietf:params:scim:api:messages:2.0:PatchOp"]
, "Operations"  : [
    { "op"      : "add"
    , "path"    : "roles"
    , "value"   : [
        { "type"  : "User"
        , "value" : 5
        , "scope" : "uid.generate"
        }
      , { "type"  : "User"
        , "value" : 5
        , "scope" : "uid.register"
        }
      ]
    }
  ]
}
```

Berechtigung entziehen

```
PATCH /Tenants/{id}
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8......
{ "schemas"     : ["urn:ietf:params:scim:api:messages:2.0:PatchOp"]
, "Operations"  : [
    { "op"      : "remove"
    , "path"    : "roles[value eq 5 and scopes eq \"uid.generate\"]"
    }
  , { "op"      : "remove"
    , "path"    : "roles[value eq 5 and scopes eq \"uid.register\"]"
    }
  ]
}
```