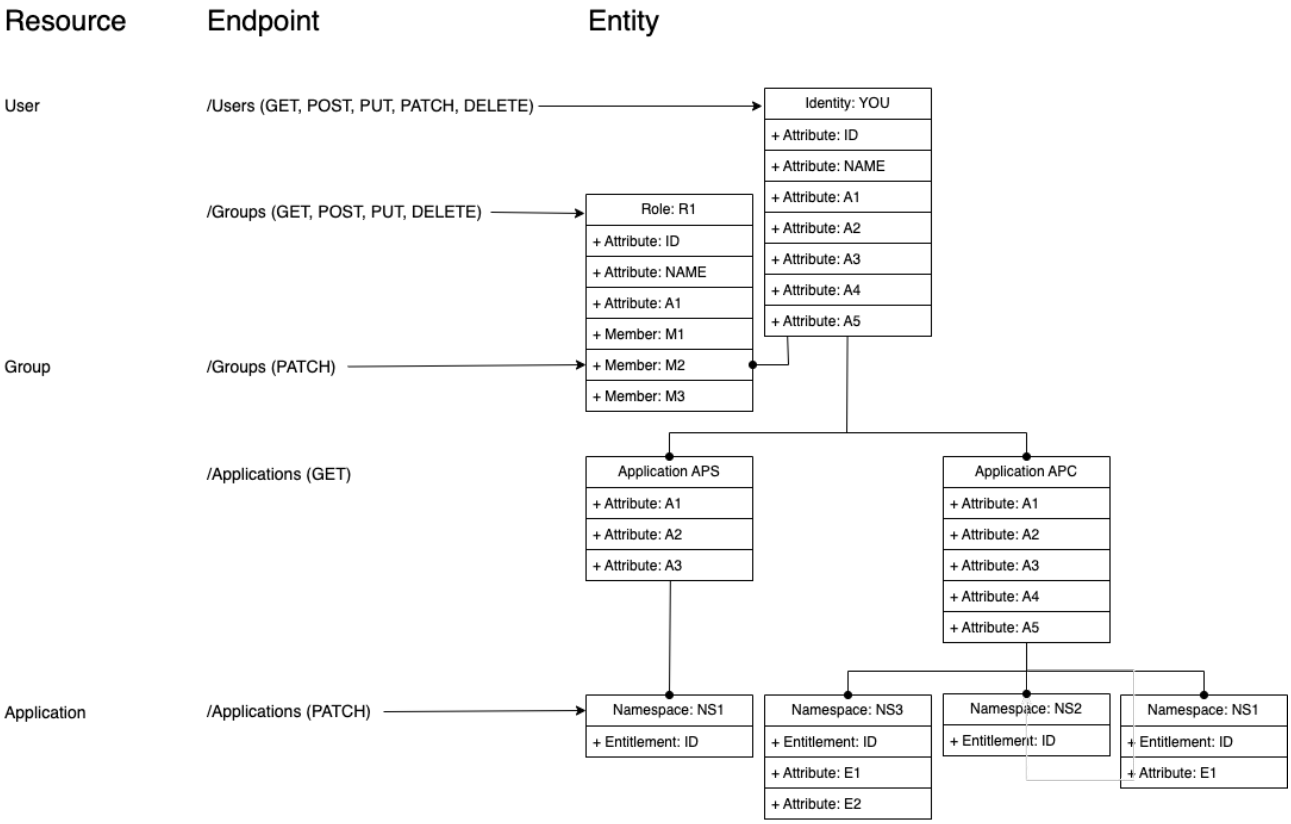
AW-Übersicht für TN-SCIMv2-Extended-v3-2024 1114_143947-1

Aktuelle Endpunkte

Resource	Enpoint	Operations
User	/Users	GET
		POST
		PUT
		PATCH
		DELETE
Group	/Groups	GET
		POST
		PUT
		PATCH
		DELETE
Application	/Applications	GET
		PATCH



Identität (Identity)

Eine Identität besteht aus einer Ansammlung von Attributen und deren Werten.

Die Verwaltung dieser Attribute über den Lebenszyklus einer Identität hinweg erfolgt über den Endpunkt */Users*.

Wesentlich ist, dass Änderungen an diesen Attributen Auswirkung auf die mit dieser Identität verbunden Applikationen haben können.
Beispiel:
Die Änderung des Attributes A1 wird entsprechend der obigen Darstellung in die Applikationen APS und APC propagiert.

Rollen (Role)

Eine Identität besteht aus einer Ansammlung von Attributen und deren Werten, sowie der Beziehung zu Identitäten.
Die Verwaltung der Attribute über den Lebenszyklus einer Rolle hinweg erfolgt über den Endpunk */Groups*.

Die Zuweisung oder der Entzug von Rollen zu und von Identitäten erfolgt über den Endpunkt */Groups* unter der Verwendung der HTTP-Methode PATCH.

Applikationen (Application)

Applikationen sind angebunden Systeme, in denen Benutzerkonten und deren Berechtigungen verwaltet werden.
Die Applikationen und deren Attribute werden durch das F-IAM vorgegeben und sind über die SCIM V2 Schnittstelle nicht veränderbar. Aus diesem Grund sind die HTTP-Methoden POST, PUT und DELETE nicht implementiert.

Die Verwaltung der Benutzerkonten erfolgt über den Endpunkt /Applications wobei die Komplexität der Anwendung darüber entscheidet, wie diese anzusteuern sind.

Die PATCH-Operation erlaubt die Manipulation der Daten von Benutzerkonten und den damit verbunden Berechtigungen in den Namensräumen der Applikation.

Diskussion

Paragraph:

„Um auf eine Anwendung zugreifen zu können, muss der Benutzer jeweils einen Account dafür eingerichtet bekommen. Dies erfolgt jeweils durch Zuweisen einer zentral eingerichteten Rolle und muss zusätzlich zum Zuweisen der AW-spezifischen Rechte geschehen“

Bemerkung:
Die Zuweisung einer Rolle ist nicht zwingend erforderlich.
Eine Rolle umfasst immer die Erzeugung eines Benutzerkontos in der/den Applikation(en) die in den Richtlinien (Policies) der Rolle definiert sind. Diese können auch Berechtigungen enthalten.
Ist in verschiedenen Rollen über die Richtlinien die gleiche Applikation aber mit unterschiedlichen Rechten spezifiziert, wird bei Zuweisung der jeweils anderen Rolle lediglich das Set an Berechtigungen manipuliert.

Applikationen:

Achtung:
Hier wird bereits die Resource **Entitlement** verwendet.
Die kommt aber noch, demzufolge wird bei einer strikten Verwendung der Semantik das zu einem Problem (HTTP 404 Not Found).
Was Tun?
Um die SCIM Konformität einzuhalten auf den Entitlements-Enpoint verzichten?
→ Damit muss immer über die Applikation navigiert werden
Oder
Den Entitlements Endpoint vorziehen?

Abfrage:

```
GET /scim/v2/Applications?startIndex=1&count=1 HTTP/1.1
User-Agent    : <User Application>
Authorization : <Authorization credentials>
Accept        : application/scim+json

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

{ "schemas"                    : [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ]
, "startIndex"                 : 1
, "totalResults"               : 3
, "itemsPerPage"               : 1
, "Resources"                  : [
    { "schemas"                : [

"urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:Application
"
      ]
```

```
    , "applicationName"          : "ZIMPAccount"
    , "namespaces"               : [
        { "namespace"            : "UD_ZIMP_UGP"
        , "entitlements"         : [
            { "entitlementName" : "ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e"
            , "attributeValues" : [
                { "attributes" : [
                  { "name"     : "Account Group"
                  , "value"    : "ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e"
                  }
                ]
               , "members"       : [
                ]
               }
              ]
            , "meta"             : {
                "resourceType" : "Entitlement"
              ,  "location"      :
"{scim-service-authority}/Entitlements/ZIMP.Endpoint~cn=ZIMP_BKA-
EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e
              }
            }
          , { "entitlementName" : "ZIMP.Endpoint~cn=ZIMP_INPOL-
F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
            , "attributeValues" : [
                { "attributes" : [
                  { "name"     : "Account Group"
                  , "value"    : "ZIMP.Endpoint~cn=ZIMP_INPOL-
F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
                  }
                ]
                , "members"      : [
                  ]
                }
              ]
            , "meta"             : {
                "resourceType" : "Entitlement"
              ,  "location"      :
"{scim-service-authority}/Entitlements/ZIMP.Endpoint~cn=ZIMP_INPOL
-F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
              }
            }
          ]
      ]
    , "meta"                       : {
        "resourceType"             : "Application"
```

```
      ,  "location"                :
"{scim-service-authority}/Applications/ZIMPAccount"
    }
  ]
}
```

Berechtigungen

Hier wird bereits die Resource **Entitlement** verwendet.

Die kommt aber noch, demzufolge wird bei einer strikten Verwendung der Semantik das zu einem Problem (HTTP 404 Not Found).

Was Tun?

Um die SCIM Konformität einzuhalten auf den Entitlements-Enpoint verzichten?

→ Damit muss immer über die Applikation navigiert werden

Oder

Den Entitlements Endpoint vorziehen?

1.1 Anbindungstyp einfach – Rechteabfrage

Change: Metadata added on all levels

```
GET /scim/v2/Applications/ZIMPAccount HTTP/1.1
User-Agent    : <User Application>
Authorization : <Authorization credentials>
Accept        : application/scim+json

HTTP/1.1 200 OK
Content-Type  : application/scim+json
{ "schemas"                 : [

"urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:Application
"
  ]
, "applicationName"         : "ZIMPAccount"
, "namespaces"              : [
    { "namespace"           : "UD_ZIMP_UGP"
    , "entitlements"        : [
        { "entitlementName" : "ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e"
        , "attributeValues" : [
            { "attributes" : [
              { "name"     : "Account Group"
              , "value"    : "ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e"
              }
            ]
          , "members"       : [
            ]
          }
        ]
```

```
        , "meta"            : {
             "resourceType" : "Entitlement"
           , "location"     :
"{scim-service-authority}/Entitlements/ZIMP.Endpoint~cn=ZIMP_BKA-
EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e
           }
         }
       , { "entitlementName" : "ZIMP.Endpoint~cn=ZIMP_INPOL-
F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
         , "attributeValues" : [
             { "attributes" : [
               { "name"     : "Account Group"
               , "value"    : "ZIMP.Endpoint~cn=ZIMP_INPOL-
F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
               }
             ]
             , "members"    : [
                 { "value"   : "userID"
                 , "type"    : "User"
                 , "$ref"    :
"{scim-service-authority}/Users/{userID}"
                 }
               , { "value"   : "userID"
                 , "type"    : "User"
                 , "$ref"    :
"{scim-service-authority}/Users/{userID}"
                 }
               , { "value"   : "userID"
                 , "type"    : "User"
                 , "$ref"    :
"{scim-service-authority}/Users/{userID}"
                 }
               ]
             }
           ]
         , "meta"            : {
             "resourceType" : "Entitlement"
           , "location"     :
"{scim-service-authority}/Entitlements/ZIMP.Endpoint~cn=ZIMP_INPOL
-F_ABGLI2,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de"
           }
         }
       ]
     , "meta"                : {
          "resourceType"     : "Namespace"
       ,  "location"         :
"{scim-service-authority}/ZIMPAccount/UD_ZIMP_UGP"
       }
     }
  ]
, "meta"                     : {
```

```
    "resourceType"            : "Application"
  ,  "location"               :
"{scim-service-authority}/Applications/ZIMPAccount"
}
```

1.2 Anbindungstyp einfach – Rechtezuweisung

Change: removed empty attribute array

```
PATCH
{scim-service-authority}/Applications/ZIMPAccount/UD_ZIMP_UGP/ZIMP
.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e
User-Agent    : <User Application>
Authorization : <Authorization credentials>
Accept        : application/scim+json
Content-Type  : application/scim+json

{ "schemas"        : [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ]
, "Operations"     : [
    { "op"         : "add"
    , "path"       : "members"
    , "value"      : [
        { "value"  : "{userid}" }
      ]
    }
  ]
}

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

1.3 Anbindungstyp einfach – Rechteentzug

Um eine Rechtezuweisung mit dem Filter „eq“ zu entfernen, wird folgendes Format für die Anforderung verwendet:

```
members[value eq \"{userid}\"]
```

Wenn eine Rechtezuweisung mit dem Filter „eq“ entfernt wird, wird den im Pfad mit dem Filter aufgelisteten Benutzerkennungen das Recht entzogen.
Andere Rechtezuweisung der Gruppe werden nicht geändert.

```
PATCH
{scim-service-authority}/Applications/ZIMPAccount/UD_ZIMP_UGP/ZIMP
.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e
{ "schemas"        : [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
```

```
  ]
, "Operations"     : [
     { "op"        : "remove"
     , "path"      : "members[value eq \"{userid}\"]"
     }
  ]
}

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

Alternativ

Wenn eine Rechtezuweisung ohne den Filter „eq“ entfernt wird, wird den unter „value“ aufgelisteten Benutzerkennungen das Recht entzogen.
Andere Rechtezuweisung der Gruppe werden nicht geändert.

```
PATCH
{scim-service-authority}/Applications/ZIMPAccount/UD_ZIMP_UGP/ZIMP
.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=d
e
{ "schemas"        : [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ]
, "Operations"     : [
     { "op"        : "remove"
     , "path"      : "members"
     , "value"     : [
         { "value" : "{userID}" }
       , { "value" : "{userID}" }
       ]
     }
  ]
}
```

Geplante Endpunkte

Resource	Enpoint	Operations
Entitlement	/Entitlemens	GET
		PATCH
Policy	/Policies	GET
		POST
		PUT
		PATCH
		DELETE
OUPermission	/OUPermissions	GET
		PATCH
		PUT
		PATCH
		DELETE