AW-Übersicht für TN-SCIMv2-Extended

IAM - Identity and Access Management

Exported on 11/14/2024

Table of Contents

Die Art, wie AW-Rechte vom F-IAM abgefragt und ihre Zuweisungen am F-IAM gepflegt werden können, hängt davon ab, wie die AWs jeweils am F-IAM angebunden sind.

Aus Sicht der Provisionierung über die TN-SCIMv2-Extended-Schnittstelle sind die folgenden **Anbindungstypen** zu unterscheiden:

- **Einfach**: Nur Rechte ohne Dienststellenbezug
- **Komplex**: Auch Rechte mit Dienststellenbezug
- **Individuell**: Individuelles IAM-Datenmodell

Der Name im F-IAM ergibt sich i.d.R. aus dem Anwendungsname mit angehängtem "Account". Über den Endpunkt Applications/<AW-ID> können die Rechte abgefragt werden.

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.

Die Rechte sind jeweils in Namespaces gruppiert. Über Applications<AW-ID>/<Recht-Namespace>/<Recht-ID> können die Rechte zugewiesen und entzogen werden.

Die ID des Rechts, über die sie im F-IAM zu referenzieren sind, ist immer `entitlementName`.

Der Name der Rechte, der zur Anzeige in der Benutzerverwaltung zu nutzen ist, kann jeweils als Attribut des Rechtes ausgelesen werden, wobei der Name des Attributs abhängig von der jeweiligen Anbindung ist.

Anwendung	AW-ID	Anbindungstyp	Rolle für Account	Rechte-Namespace	Attribut für Namen
ZIMP	ZIMPAccount	Einfach	?	UD_ZIMP_UGP	Account Group
IDS	IDSAccount	Einfach	?	UD_IDS_GRP	Group Name
eFBS	-	individuell	?	-	-

1 Beispiele

1.1 Anbindungstyp einfach – Rechteabfrage


```
{
    "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=de",
                    "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=de"
                                }
                            ],
                            "members": []
                        }
                    ]
                },
                {
                    "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": []
                        }
                    ]
                },
```

```
                ...
            ]
        }
    ]
}
```

1.2 Anbindungstyp einfach – Rechtezuweisung

```
PATCH /ZIMPAccount/UD_ZIMP_UGP/ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op": "add",
      "path": "members",
      "value": [
        {
          "attributes": [],
          "value": "by04765432"
        }
      ]
    }
  ]
}
```

1.3 Anbindungstyp einfach – Rechteentzug

```
PATCH /ZIMPAccount/UD_ZIMP_UGP/ZIMP.Endpoint~cn=ZIMP_BKA-EWO-
XMELD_MELDEDATEN,ou=Groups,ou=ZIMP,cn=Services,dc=bka,dc=bund,dc=de
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:PatchOp"
  ],
  "Operations": [
    {
      "op"   : "remove",
      "path" : "members[value eq \"by04765432\"]"
    }
  ]
}
```

1.4 Anbindungstyp komplex – Rechteabfrage

```
{
    "schemas": [
        "urn:ietf:params:scim:schemas:extension:oracle:2.0:OIG:Application"
    ],
    "applicationName": "ArtusAccount",
    "namespaces": [
        {
            "namespace": "UD_ARTUS_OUPERMISSION",
            "entitlements": [
                {
                    "entitlementName": "ARTUS.Endpoint~Recht1",
                    "attributeValues": [
                        {
                            "attributes": [
                                {
                                    "name": "Name",
                                    "value": "Artus.Endpoint~Recht eins"
                                },
                                {
                                    "name": "details",
                                    "value": "{ \"flags\": [\"ANY_FLAG\"] }
                                }
                            ],
                            "members": []
                        }
                    ]
                },
                ...
            ]
        }
    ]
}
```

1.5 Anbindungstyp komplex – Rechtezuweisung ohne Dst-Bezug

```
...
```

1.6 Anbindungstyp komplex – Rechtezuweisung ohne Dst-Bezug

...

1.7 Anbindungstyp komplex – Rechtezuweisung mit Dst-Bezug

...

1.8 Anbindungstyp komplex – Rechtezuweisung mit Dst-Bezug

...