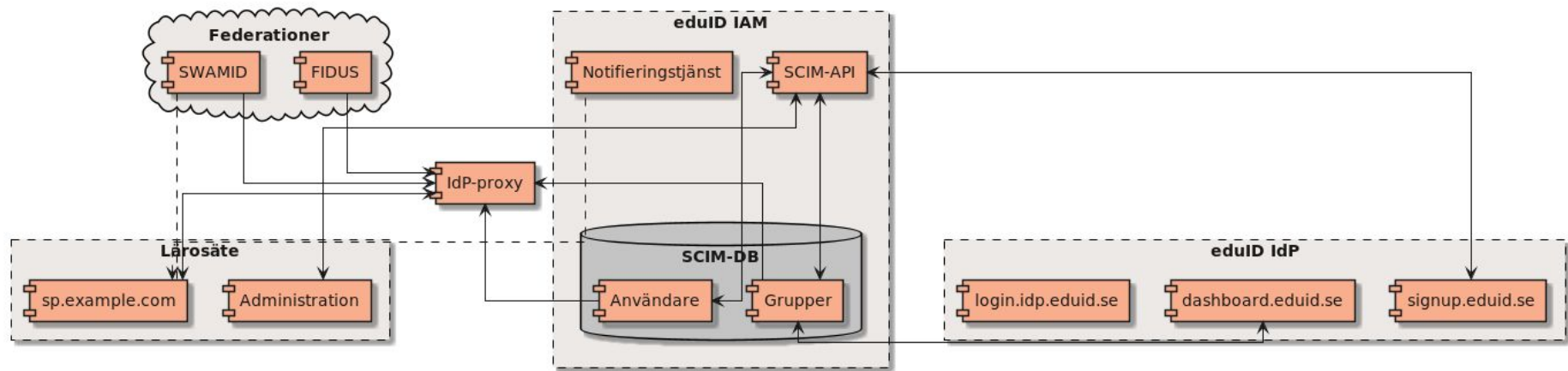


eduID IAM backend

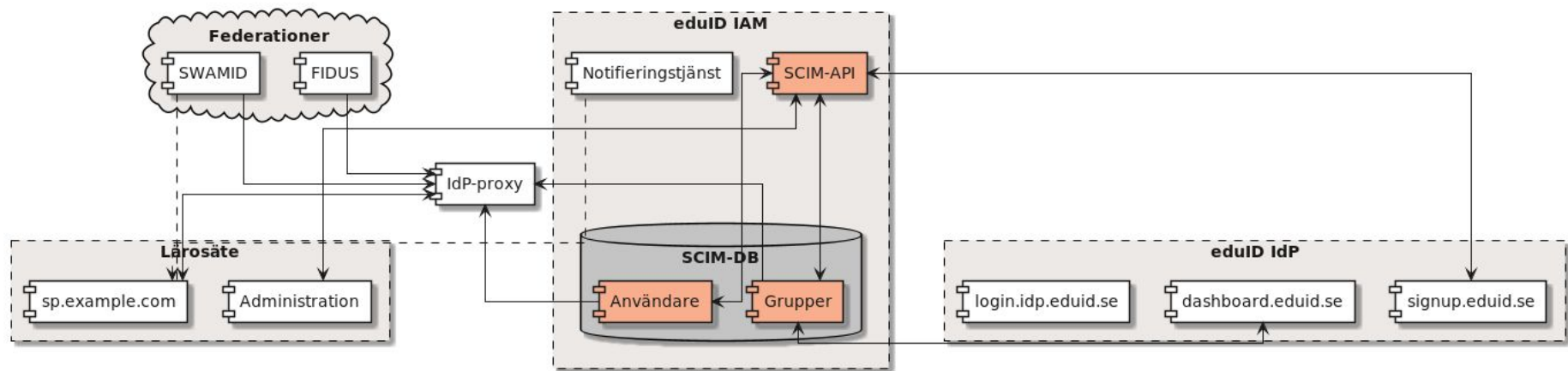


Översikt



SCIM-API

SCIM-API



SCIM User Resource

```
{
  "externalId": "rabog-zorul@eduid.se",
  "groups": [
    {
      "$ref": "http://scimapi.eduid.docker:8000/Groups/fe54dc67-ac7b-42b9-a9e9-105a9e03d72f",
      "display": "Test Group 1",
      "value": "fe54dc67-ac7b-42b9-a9e9-105a9e03d72f"
    }
  ],
  "id": "232fd0df-3223-4117-8783-5706038bc6c0",
  "meta": {
    "created": "2020-05-14T15:14:27.132000+00:00",
    "lastModified": "2020-10-16T13:25:24.492560",
    "location": "http://scimapi.eduid.docker:8000/Users/232fd0df-3223-4117-8783-5706038bc6c0",
    "resourceType": "User",
    "version": "W/\ "5f899f44e3e8d25da5d4288a\ "
  },
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ]
}
```

SCIM Group Resource

```
{
  "displayName": "Test Group 1",
  "id": "fe54dc67-ac7b-42b9-a9e9-105a9e03d72f",
  "members": [
    {
      "$ref": "http://scimapi.eduid.docker:8000/Users/232fd0df-3223-4117-8783-5706038bc6c0",
      "display": "Member 1",
      "value": "232fd0df-3223-4117-8783-5706038bc6c0"
    }
  ],
  "meta": {
    "created": "2020-05-06T09:07:07.104000+00:00",
    "lastModified": "2020-05-14T15:15:19.537000+00:00",
    "location": "http://scimapi.eduid.docker:8000/Groups/fe54dc67-ac7b-42b9-a9e9-105a9e03d72f",
    "resourceType": "Group",
    "version": "W/\\"5ebd60878c06841a5ba78f45\\"
  },
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group"
  ]
}
```

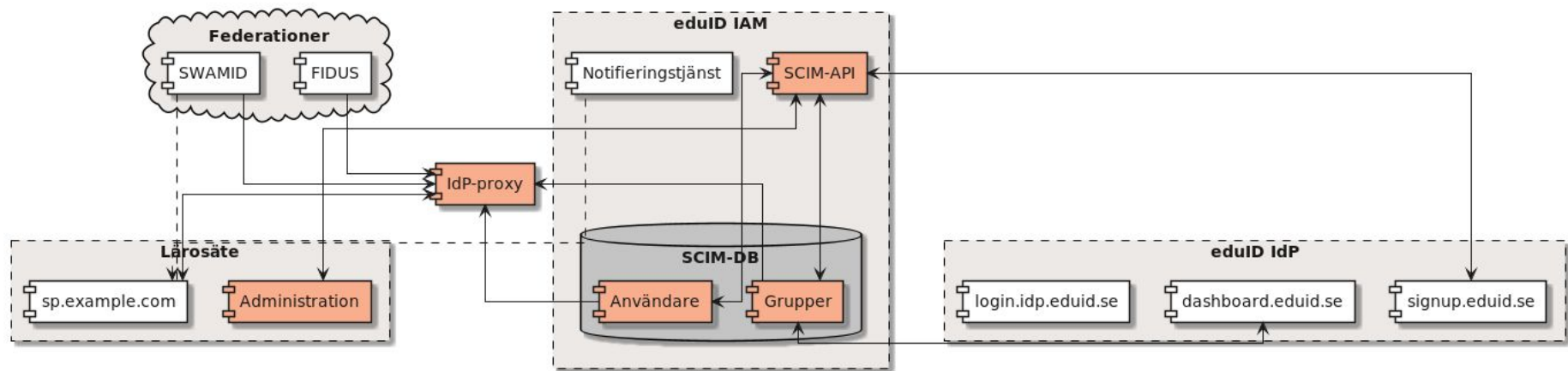
SCIM Extensions

```
{
  "externalId": "rabog-zorul@eduid.se",
  ...
  "https://scim.eduid.se/schema/nutid/user/v1": {
    "profiles": {
      "other_profile": {
        "attributes": {
          "displayName": "K. Anka"
        },
        "data": {}
      },
      "student": {
        "attributes": {
          "displayName": "Anders And"
        },
        "data": {
          "test_key": "ett värde"
        }
      }
    }
  },
  ...
  "id": "232fd0df-3223-4117-8783-5706038bc6c0",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "https://scim.eduid.se/schema/nutid/user/v1"
  ]
}
```

```
{
  "displayName": "Test Group 1",
  "id": "fe54dc67-ac7b-42b9-a9e9-105a9e03d72f",
  ...
  "https://scim.eduid.se/schema/nutid/group/v1": {
    "data": {
      "test_key": "foo"
    }
  },
  ...
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group",
    "https://scim.eduid.se/schema/nutid/group/v1"
  ]
}
```

Dataägarmodell

Dataägarmodell

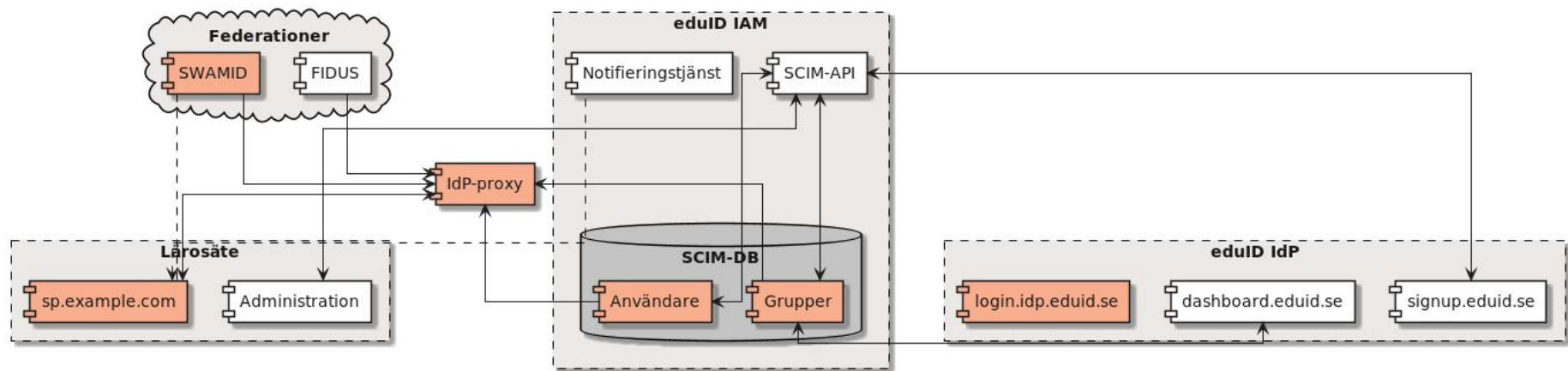


Dataägarmodell

- Varje lärosäte har en “partition” i SCIM-databasen, vilken man kommer åt via SCIM-API:et

IdP-proxy

IdP-proxy



IdP-proxyns funktion

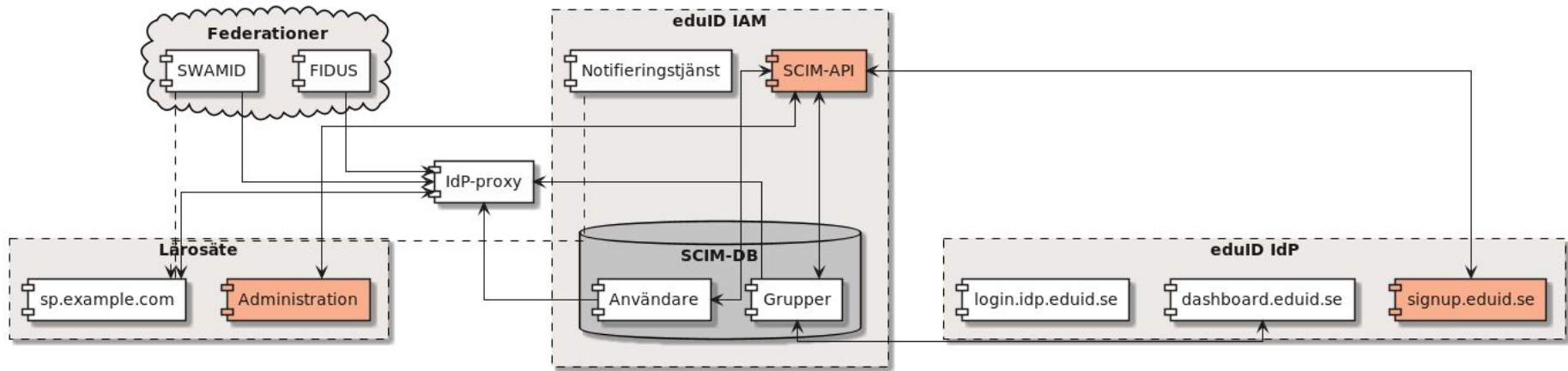
- IdP-proxyn modifierar SAML-biljetten baserat på vilken “backend-IdP” som används, och backend-IdP:n hör till lärosätets partition

Användningsfall för en IdP-proxy

- Exponera gruppmedlemskap från eduID IAM till en SP
- Förbehandla data åt en SP som kanske inte förstår federationer
- Fylla på en SAML-biljett med attribut som inte går att få in i en viss IdP
- Step-up autentisering med andra faktor (MFA)

eduID SCIM-inbjudan

eduID SCIM-inbjudan

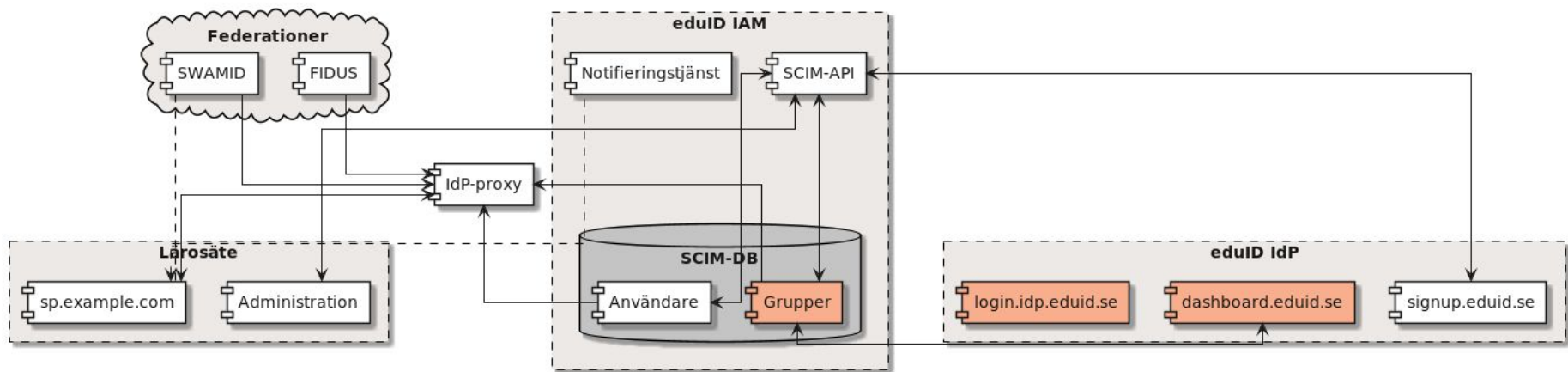


eduID SCIM-inbjudan

- Ett sätt för ett lärosäte att bidra med redan känd information om användare, för att göra sign-up enklare.
- I förlängningen en viktig pusselbit för att göra virtuella idp:er åt lärosäten som önskar det.
- Åtkomlig som en SCIM extension i SCIM-API:t, för enkelhetens skull

Grupper i eduID IdP

Grupper i eduID IdP

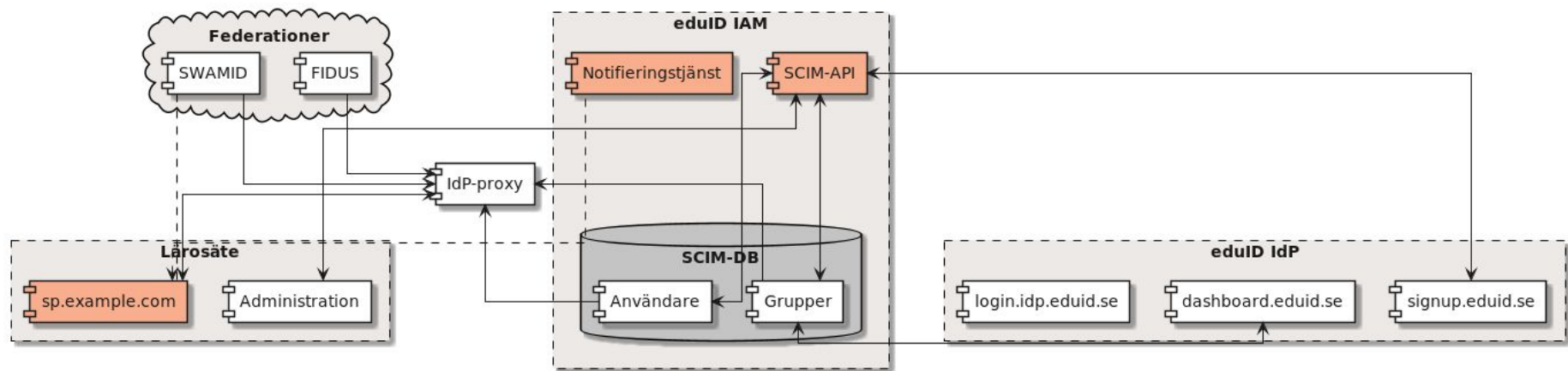


Grupper i eduID IdP

- För personliga grupper (eduID IdP) kommer det finnas ett UI i eller kopplat till eduID IdP dashboard
- Roller: Ägare, medlem eller både och
- Bjud in personer via e-post, de bekräftar i eduID IdP dashboard
- Institutionella grupper (eduID IAM) kommer administreras i ett annat interface, ej påbörjat

Notifieringstjänst

Notifieringstjänst



Notifieringstjänst

- Rapporterar skapade, ändrade eller borttagna objekt
- Skickar bara referenser till påverkade objekt
- Första version baserad på Amazon Simple Notification Service
- Bygger intern kö för att ersätta Celery baserad på MongoDB

Källkod

SCIM-API

<https://github.com/sunet/eduid-scimapi>

Gruppdatabas

<https://github.com/sunet/eduid-graphdb>

IdP-proxy (satos)

<https://github.com/identitypython/satos>

MongoDB-baserad kö (tidig utveckling)

<https://github.com/sunet/eduid-queue>