Rollekataloget

Anvendelse af AD Sync Service

Version: 1.3.0
Date: 02.02.2021
Author: BSG

Indhold

1 Indledning 3
1.1 Forudsætninger 3
2 Installation 3
3 Konfiguration 3
3.1 CronSchedule 3
3.2 ApiUrl og ApiKey 3
3.3 CreateDelete feature 4
3.4 MembershipSync feature 4
3.5 BackSync feature 5
3.6 ItSystemGroup feature 5

1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og ADSyncService.

1.1 Forudsætninger

Der installeres en Windows Service der afvikler ADSyncService integrationen. Denne skal afvikles under en systemkonto der har de fornødne rettigheder, dvs

- Lov til at melde brugere ind/ud af AD grupper
- Lov til at oprette/nedlægge AD grupper (hvis integrationen også skal gøre dette)

2 Installation

Løsningen kommer som en EXE installer, der blot skal afvikles. Dette sikrer at løsningen installeres på den valgte server, og at der opsættes en Windows Service.

Herefter skal man, under services, vælge at servicen skal afvikles under den systemkonto der har de nævnte rettigheder.

Endeligt skal løsningen konfigureres som beskrevet nedenfor, før selve servicen startes.

3 Konfiguration

Efter installationen ligger der en konfiguratiosnfil i installationsfolderen. Denne skal tilpasses. Navnet på filen er

`ADSyncService.exe.config`

Filen indeholder følgende settings

3.1 CronSchedule

Dette er hvor ofte integrationen skal afvikles. Det anbefales at efterlade den med default værdien, som er hvert 5. minut

```
<setting name="CronSchedule" serializeAs="String">
  <value>0 /5 * ? * *</value>
</setting>
```

3.2 ApiUrl og ApiKey

Dette er hhv URL til rollekataloget, og den nøgle der skal bruges til at tilgå rollekataloget. Disse kan udlevers af driftoperatøren. Værdierne SKAL udfyldes.

```
<setting name="ApiUrl" serializeAs="String">
  <value>https://kommune.rollekatalog.dk</value>
</setting>
<setting name="ApiKey" serializeAs="String">
  <value>xxxxxxxxxxxxxxxxxxxxxxxxxxx</value>
</setting>
```

3.3 CreateDelete feature

Man kan vælge at ADSyncService også skal oprette/nedlægge AD grupper (på bestilling inde fra OS2rollekatalogs brugergrænseflade). Dette kræver at nedenstående features er enabled. Default er det slået fra via hoved-settingen (CreateDeleteFeature_Enabled), som man skal ændre til "True" hvis denne funktion ønskes. Man kan også vælge at slå create/delete til individuelt, men hovedsettingen skal dog altid være slået til for at disse virker.

Hvis man har valg at featuren skal være slået til, så SKAL man udfylde CreateDeleteFeature_OU med en pegepind (et DN) på den OU i AD hvor grupperne skal oprettes.

```
<setting name="CreateDeleteFeature_Enabled" serializeAs="String">
  <value>False</value>
</setting>
<setting name="CreateDeleteFeature_CreateEnabled" serializeAs="String">
  <value>True</value>
</setting>
<setting name="CreateDeleteFeature_DeleteEnabled" serializeAs="String">
  <value>True</value>
</setting>
<setting name="CreateDeleteFeature_OU" serializeAs="String">
  <value>OU=groups,DC=digitalidentity,DC=dk</value>
</setting>
```

3.4 MembershipSync feature

Dette er den primære funktion i servicen, og den er slået til som default. Det er denne indstilling som sikrer at brugere meldes ind/ud af grupper i AD på baggrund af rolletildelinger i OS2rollekatalog.

Som default ignoreres alle brugere der ikke har et CPR nummer udfyldt, og man skal angive hvilken attribut som CPR nummeret kan læses i (hvis feltet er beskyttet skal servicekontoen have adgang til feltet).

```
<setting name="MembershipSyncFeature_Enabled" serializeAs="String">
  <value>True</value>
</setting>
<setting name="MembershipSyncFeature_IgnoreUsersWithoutCpr"
serializeAs="String">
  <value>True</value>
```

```
      </setting>
      <setting name="MembershipSyncFeature_CprAttribute" serializeAs="String">
        <value>employeeNumber</value>
      </setting>
```

3.5 BackSync feature

Denne feature opretter roller og nedlægger roller i OS2rollekatalog på baggrund af eksistensen af AD grupper. Featuren er som udgangspunkt slået fra, og kan slås til ved at sætte værdien til "True".

Hvis den er slået til, skal man angive en mapningstabel mellem ID'er på it-systemer i OS2rollekatalog og OU'ere i AD'et.

Alle grupper der ligger i den/de angivne OU'ere, bliver synkroniseret til OS2rollekatalog som systemroller og jobfunktionsroller. Medlemsskaber skal vedligeholdes fra OS2rollekatalog, men på denne måde kan man automatisk få indlæst AD grupper fra en OU, uden at skulle oprette dem manuelt.

Bemærk at synkroniseringen KUN kan lade sig gøre for it-systemer hvor man har slået "vedligehold via API" til inde i OS2rollekatalog (rediger it-systemet og sæt flueben i dette felt).

```
      <setting name="BackSyncFeature_Enabled" serializeAs="String">
        <value>False</value>
      </setting>
      <setting name="BackSyncFeature_OUs" serializeAs="Xml">
        <value>
          <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <string>2399;OU=system1,OU=Groups,DC=digitalidentity,DC=dk</string>
            <string>2400;OU=system2,OU=Groups,DC=digitalidentity,DC=dk</string>
          </ArrayOfString>
        </value>
      </setting>
```

3.6 ItSystemGroup feature

Denne feature kan bruges til at vedligeholde AD grupper, der repræsentere et helt it-system. Brugere som har bare én rolle i et it-system vil blive meldt ind i den angive AD gruppe. Som ved den forrige feature, skal der opsættes en mapningstabel mellem it-systemet (via dets ID) og den gruppe i AD der skal meldes brugere ind/ud af.

```
      <setting name="ItSystemGroupFeature_Enabled" serializeAs="String">
        <value>False</value>
      </setting>
      <setting name="ItSystemGroupFeature_SystemMap" serializeAs="Xml">
        <value>
          <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <string>1;CN=ItSystemOne,OU=Groups,DC=digitalidentity,DC=dk</string>
          </ArrayOfString>
        </value>
      </setting>
```