

Rollekataloget

Anvendelse af AD Sync Service

Version: 2.1.0
Date: 11.03.2023
Author: PSO

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	Domæne – optionelt	4
3.4	CreateDelete feature	4
3.5	MembershipSync feature	5
3.6	BackSync feature	6
3.7	ItSystemGroup feature.....	7
3.8	ReadOnly feature	7

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 CreateDelete feature anvendes)
- Lov til at oprette/nedlægge OU'er (hvis CreateDelete feature anvendes)

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 konfigurationsfil 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 alle dagens timer mellem kl 5 og 23.

```
<setting name="CronSchedule" serializeAs="String">  
  <value>0 /5 5-23 ? * *</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 udleveres af driftoperatøren. Værdierne SKAL udfyldes.

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

```
</setting>
```

Man kan danne en API nøgle i rollekataloget. Det gøres på følgende måde:

- Log ind på rollekataloget
- Tryk på "Administration" i top-menuen
- Tryk på "Klienter" i venstre-menuen
- Tryk på "Opret klient"-knappen, der vises i toppen af siden
- Giv klienten et navn
- Vælg om du vil bruge den API nøgle, der er dannet, eller om du vil lave din egen
- Vælg adgangen "Rolleadministration"
- Tryk på "Gem"-knappen.
- Du kan nu bruge API nøglen fra den klient, du har lavet.

3.3 Domæne – optionelt

Hvis man kører med opsplittede domæner i indlæsningen til OS2rollekatalog, så kan man angive en optionel domæneparameter (hvis man ikke gør, så indlæses data i det normale/primære domæne). Denne værdi sættes til "skole" for skole-domænet, hvilket er den tiltænkte anvendelsen af denne setting.

```
<setting name="Domain" serializeAs="String">  
  <value>skole</value>  
</setting>
```

3.4 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>
```

3.5 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>
```

Det er også muligt at indlæse en konfigurerbar værdi i en eller flere AD attributter på brugerne som meldes ind i en adgruppe via denne feature.

```
<setting name="MembershipSyncFeature_AttributeMap" serializeAs="Xml">
  <value>
    <ArrayOfString xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <string>someGroupName;someAttribute;someAttributeValue</string>
    </ArrayOfString>
  </value>
</setting>
```

3.6 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.

Endeligt kan man angive om der automatisk skal oprettes Jobfunktionsroller for hver systemrolle der indlæses, dette gøres via BackSyncFeature_CreateUserRoles, som i så fald sættes til "True" (dette er default).

Alle grupper der ligger i den/de angivne OU'ere, bliver synkroniseret til OS2rollekatalog som systemroller (og jobfunktionsroller hvis det er slået til ovenfor).

Første gang en AD gruppe indlæses i OS2rollekatalog, så hentes også alle brugere med (kun hvis Jobfunktionsroller også oprettes). Hermed sikres det at brugere der allerede er medlem af gruppen bliver tildelt den tilsvarende Jobfunktionsrolle fra start.

Medlemsskaber skal efterfølgende 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_CreateUserRoles" serializeAs="String">
  <value>True</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>
```

3.7 ItSystemGroup feature

Denne feature kan bruges til at vedligeholde AD grupper, der repræsenterer et helt it-system. Brugere som har bare én rolle i et it-system vil blive meldt ind i den angivne 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.

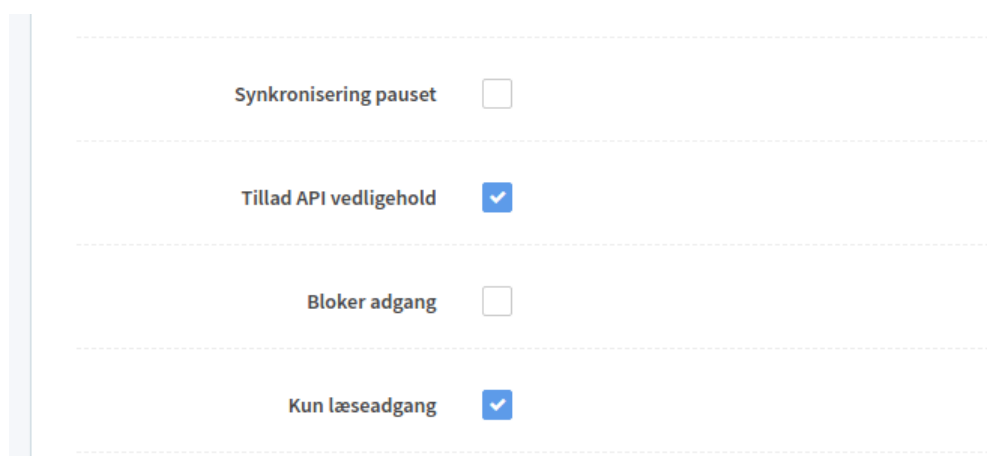
```
<setting name="ItSystemGroupFeature_Enabled" serializeAs="String">
  <value>False</value>
</setting>

<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>
```

3.8 ReadOnly feature

Denne feature bruges til at dokumentere AD grupper i OS2rollekatalog, hvor man ønsker at it-systemet skal vedligeholdes i AD, men blot afspejles i OS2rollekatalog.

Denne feature (modsat de andre) tillader at ændringer i gruppemedlemsskaber foretaget i AD bliver afspejlet i OS2rollekatalog. For at sikre at der ikke opstår konflikt mellem OS2rollekatalog og AD, kan denne funktion KUN opsættes for it-systemer som har "read-only" flagget sat inde i OS2rollekatalog, som vist nedenfor



Synkronisering pauset	<input type="checkbox"/>
Tillad API vedligehold	<input checked="" type="checkbox"/>
Bloker adgang	<input type="checkbox"/>
Kun læseadgang	<input checked="" type="checkbox"/>

Bemærk her at både "Tillad API vedligehold" og "Kun læseadgang" skal være slået til på it-systemet.

Som for BackSync features skal der vedligeholdes en liste af mapninger mellem ID'erne på it-systemer i rollekataloget og den OU hvor de tilsvarende AD grupper er placeret

```
<setting name="ReadonlyItSystemFeature_SystemMap" serializeAs="Xml">
  <value>
    <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <string>2408;OU=system1,OU=Groups,DC=digitalidentity,DC=dk</string>
      <string>2409;OU=system2,OU=Groups,DC=digitalidentity,DC=dk</string>
    </ArrayOfString>
  </value>
</setting>
```

Endeligt skal selve features været slået til

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