OS2syncAD

Installationsvejledning

Version: 4.4.0
Date: 13.09.2024
Author: BSG

Indholdsfortegnelse

1 Indledning

Formålet med dokument er at dække installation og konfiguration af OS2sync synkroniseringsmodulet, der kan synkronisere organisationsdata fra Active Directory, til FK Organisation.

2 Installation

2.1 Forudsætninger

For at kunne anvende softwaren, er der en række forudsætninger der skal være på plads. Disse er

2.1.1 Et OCES3 certifikat

For at anvende løsningen, skal der bruges et OCES3 certifikat, som er krævet for at kalde organisationsservicen.

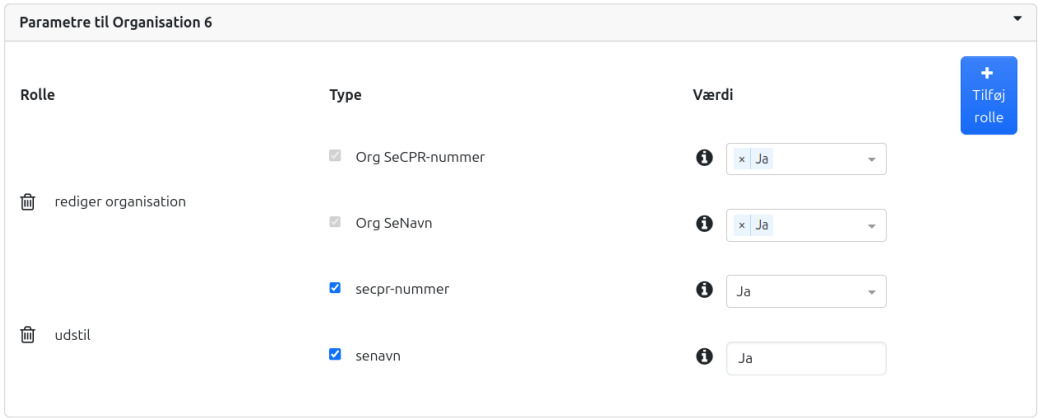
2.1.2 Serviceaftale på støttesystemerne

Der skal være oprettet (og godkendt) en serviceaftale på støttesystemet Administrationsmodul, hvor der er givet skriveadgang til FK Organisation. Denne serviceaftale skal være knyttet til det OCES3 certifikat der er nævnt ovenfor.

Serviceaftalen oprettes på følgende måde

1. Log på KOMBITs Adminisrationsmodul (https://admin.serviceplatformen.dk)
2. Opret et nyt it-system af typen Anvendersystem, og upload OCES3 certifikatet som en del af registreringen
3. Anmod om en serviceaftale, hvor der vælges "Organisation 6" som service
4. Både "udstil" og "rediger organisation" rollerne skal vælges, og alle dataafgrænsinger tilvælges med værdien Ja

Husk at få godkendt serviceaftalen.



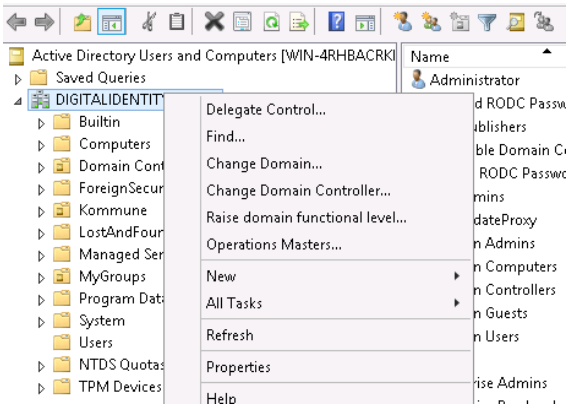
2.1.3 Windows Server og systembruger konto

Softwaren skal installeres på en Windows Server (2016 eller nyere), og der skal være oprettet en systembruger der kan afvikle softwaren.

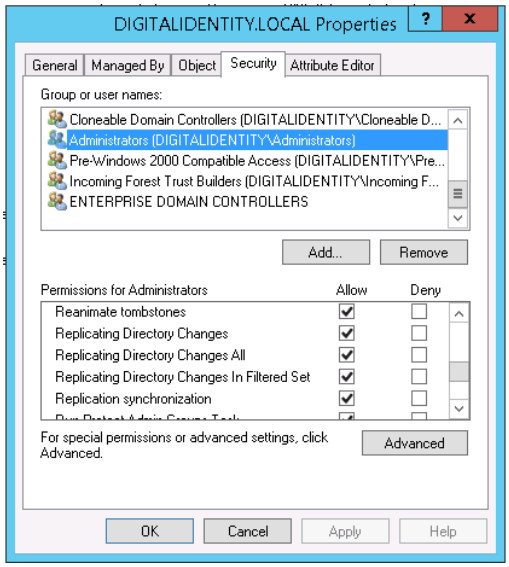
Denne systembruger skal have lokale adminsitratorrettigheder på den server hvor softwaren skal installeres.

Endelig skal systembrugeren også have rettigheder til at replikere data fra Active Directory. Dette vil brugeren automatisk have hvis denne er domæne administrator, men man kan også nøjes med at tilføje enkelte replikerings-rettigheder til brugeren via nedenstående vejledning

1. Åben "Active Directory Users and Computers" konsollen
2. Vælg domænet, højreklik, og vælg "properties"



3. Gå til security fanen, tilføj systembrugeren, og giv brugeren følgende replikeringsrettigheder (som vist i screenshottet nedenfor). Bemærk at den første formodentligt er den eneste der er nødvendig (alt afhængig af hvilke attributter der skal synkronisers)
    a. Replicating Directory Changes
    b. Replicating Directory Changes All (kun nødvendigt hvis der skal replikeres hemmelige attributter)
    c. Replicating Directory Changes In Filtered Set (kun nødvendigt hvis attributer der skal synkroniseres er beskyttede)



Bemærk at der kan gå nogle minutter fra denne rettighed er sat, til den slår igennem. Hvis man under kørsel af softwaren får "Access Denied" i loggen i kaldet til Active Directory, så er det disse synkroniseringsrettigheder der mangler.

2.1.4 SQL Server

OS2sync skal have adgang til en MS SQL server, hvor den kan gemme de data der skal overføres til FK Organisation.

Opret en database på serveren, og giv den servicekonto som skal køre OS2sync adgang til at skrive, læse og oprette tabeller på databasen.

2.2 Installation

Installationen foretages ved at køre en Windows Installer ved navn

`OS2syncADSetup.exe`

Der opsættes en Service på Windows Serveren, som dog ikke startes automatisk. Dette skal først gøres efter konfigurationen er gennemført.

Softwaren installeres som default til følgende folder (alternativ folder kan vælges under installationen)

`C:\Program Files (x86)\Digital Identity\OS2syncAD`

2.3 Konfiguration

Konfiguration af løsningen sker via filen appsettings.json. Start med at udfylde denne setting med kommunens CVR nummer

```
/* set to CVR of municipality */
"Cvr": "12345678",
```

Dernæst skal man hente de offentlige certifikater til hhv FK Organisation og KOMBITs token service (STS'en). De publiceres på digitaliseringskataloget, men for at gøre det nemt, ligger der også en kopi på www.os2sync.dk, hvor de relevante certifikater ligger i en zip fil.

Kopier filerne ind på serveren, fx under c:\certifikater, og ret så disse to indstillinger så de peger på de relevante certifikater (der er forskellige certifikater til hhv TEST og PROD)

```
/* point to file containing STS certificate */
"StsSettings": {
  "StsCertificateLocation": "c:/certifikater/sts.cer"
},

/* point to file containing FK Organisation certificate */
"ServiceSettings": {
  "WspCertificateLocation": "c:/certifikater/organisation.cer"
},
```

Det OCES3 certifikat (p12 filen) som man har fået registreret inde i KOMBITs administrationsmodul skal nu kopieres ind på serveren (fx under c:\certifikater), og så skal nedenstående konfigurationssetting tilpasses med placering og kodeord til filen

```
/* point to file (and password) for OCES 3 certificate */
"ClientSettings": {
  "WscKeystoreLocation": "c:/certifikater/keystore.p12",
  "WscKeystorePassword": "Hemmelig"
},
```

Så skal der angives adgang til den SQL server der er nævnt under forudsætninger, hvilket gøres med nedenstående indstillinger. Den præcise værdi til DBConnectionString afhænger af placeringen af SQL serveren (.\\sqlexpres rettes til et servernavn, fx "srv-sql01" eller hvad nu ens SQL server hedder)

```
  /* setup connection string */
  "SchedulerSettings": {
    "Enabled": true,
    "DBConnectionString": "server=.\\sqlexpress;Integrated
Security=true;Database=os2sync",
    "DBType": "MSSQL"
  },
```

Hvis man ønsker at OS2sync skal udføre en ugentlig oprydning i FK Organisation, kan man slå dette job til ved at ændre nedenstående indstillinger til det viste

```
  /* weekly job that removes OUs from FK Organisation that no longer exists in Active
Directory */
  "CleanupOUJobEnabled": "true",
  "CleanupOUJobDryRun": "false",
  "CleanupOUJobCron": "0 30 3 ? * FRI",
```

Så er der selve mapningen af data fra AD, hvilket gøres ved at rette følgende settings

```
    /* OU in AD from which the organisation is synchronized */
    "RootOU": "OU=Kommune,DC=digitalidentity,DC=dk",
```

Ovenstående skal pege på "roden" af den enhed i AD man ønsker at synkronisere fra. I forhold til enheder, så kan man udvælge hvilke attributter på OU'erne i AD, som skal overføres til FK Organisation via disse indstillinger (bemærk at Filter funktionen er speciel, og er beskreve længere nede)

```
    /* OU fields mapped to FK Organisation */
    "OrgUnitAttributes": {
      "Filtered": "admindescription",
      "Ean": "",
      "Email": "",
      "LOSShortName": "",
      "LOSId": "",
      "DtrId": "",
      "PayoutUnitUuid": "",
      "Phone": "telephoneNumber",
      "Post": "",
      "Name": "",
      "Location": "",
      "Contact": "",              /* Henvendelsessted */
      "ContactOpenHours": "",
      "EmailRemarks": "",
      "PostReturn": "",
      "PhoneOpenHours": "",
      "Url": "",
      "Landline": ""
    },
```

Tilsvarende kan man mappe felter fra brugerkonti via disse indstillinger

```
/* user fields mapped to FK Organisation */
"UserAttributes": {
  "Location": "",
  "Mail": "mail",
  "RacfId": "",
  "Cpr": "employeeNumber",
  "Name": "name",
  "Phone": "telephoneNumber",
  "PositionName": "title"
}
```

2.3.1 Filterfunktionen

Hvis man udfylder feltet "Filtered" i OU indstillingerne, fx som vist nedenfor

```
  "Filtered": "admindescription",
```

Så kan man udfylde det angive felt i OU'erne med enten værdien "1" eller værdien "2" hvis man ønsker at disse enheder skal filtreres væk. Hvis man angiver "1", så filtreres enheden væk, men alle de underliggende enheder kommer stadig med over i FK Organisation. Hvis man angiver "2" så ryger enheden og alle underliggende enheder væk i FK Organisation.

3 Logfiler

I konfigurationsfilen er der angivet placeringen af loggen, og ret evt defaultværdien til en anden placering, hvis den ønskes skrevet til et andet sted

```
/* configure logfile */
"LogSettings": {
  "LogFile": "c:/logs/os2sync.log",
  "LogLevel": "INFO"
},
```

Logfilen logger ganske få data under normal kørsel (hver gang der synkroniseres data, kommer en række der fortælle hvor mange data der er synkroniseret – hvis der ikke er nogen data, logges intet).

I tilfælde af fejl, logges fejlen til denne fil, og det anbefales at man, i det mindste i starten, holder øje med evt synkroniseringsfejl i denne fil.

Specielt under installationen kan det være nødvendigt at kigge i logfilen hvis der opstår fejl. Man vil typisk kunne se om der er tale om manglende rettigheder, manglende serviceaftale eller lignende ud fra fejlbeskden. En let måde at slippe udenom mange af de rettighedsudfordringer man kan støde på, er at gøre systembrugeren der afvikler servicen til lokal administrator på serveren.

Bemærk at der under den initielle synkronisering af data (første gang man kører), er rigtigt mange data der skal synkroniseres, og man skal forvente at det kan tage 4-8 timer at gennemføre en fuld synkronisering af data. Hold periodisk øje med logfilen i denne

opstartsperiode, for at se om status er som forventet (der synkronisers op til 500 enheder/medarbejdere per log-linje).

4 Håndtering af konfigurationsændringer

Hvis man ændrer i konfiguration i registreringsdatabasen, er det nødvendigt at genstarte servicen før disse ændringer slå igennem. Dette gøres via Services på Windows Servicen, hvor man blot trykker på ”restart” ud for OS2syncAD servicen.

Hvis man ændrer i hvilke AD attributter der skal synkroniseres, så er det nødvendig at tvinge en fuld synkronisering igennem. Dette tager igen de 4-8 timer.

En fuld synkronisering kan gennemtvinges på følgende måde

1. stop servicen
2. foretag de ønskede ændringer i konfigurationsfilen
3. find ”records” tabellen i SQL databasen, og slet indholdet af tabellen (slet alle rækker)
4. genstart servicen

5 Opdatering fra version 2.9

Der kan ikke opdateres fra version 2.9 til version 4.x

I stedet skal version 2.9 afinstalleres, og version 4.x skal installeres som en frisk installation. Konfigurationsfil, certifikat, serviceaftale og SQL adgang skal opsættes på frisk.

6 Opdatering fra version 4.1.x

I version 4.4.0 er der tilføjet en ny konfigurationsindstilling. Den er default med i konfigurationsfilen ved en ny installation, men ved en opdatering tilføjes den ikke som standard. Tilføj derfor denne konfigurationslinje

```
"PassiverAndReImportOnErrors": "false",
```

Hvis man oplever at objekter i FK Organisation ikke kan opdateres, pga fejl på adresser eller andre relationer, så kan man vælge at ændre ovenstående indstilling til ”true”. Så vil OS2sync, hvis der opstår sådanne fejl, nulstille objektet helt i FK Organisation, og så lave en gen-import af dataene.