OS2nykode

Installation og konfiguration

**Date**: 28.02.2020

**Author**: BSG

Indhold

[1 Indledning 3](#_Toc32559977)

[2 Forudsætninger 3](#_Toc32559978)

[2.1 Docker 4](#_Toc32559979)

[2.2 NemID tjensteudbyderaftale 4](#_Toc32559980)

[2.3 Familie servicen 4](#_Toc32559981)

[2.4 SMS Gateway 4](#_Toc32559982)

[2.5 MySQL 5](#_Toc32559983)

[2.6 UniLogin 5](#_Toc32559984)

[2.7 AD (AD FS) login til OS2nykode 5](#_Toc32559985)

[3 Konfiguration 6](#_Toc32559986)

[3.1 Miljø-parametre 6](#_Toc32559987)

[3.1.1 Miljø parametre for SMS modulet 6](#_Toc32559988)

[3.1.2 Miljø parametre for Familie modulet 6](#_Toc32559989)

[3.1.3 Miljø parametre for OS2nykode grundmodulet 7](#_Toc32559990)

[3.2 Password politikker 11](#_Toc32559991)

[4 Eksempel Docker Compose fil 12](#_Toc32559992)

[5 Docker kommandoer 14](#_Toc32559993)

[5.1 Starte og/eller genstarte applikationen 14](#_Toc32559994)

[5.2 Se alle kørende containere 14](#_Toc32559995)

[5.3 Se loggen fra en container 14](#_Toc32559996)

[5.4 Stoppe en container 15](#_Toc32559997)

[5.5 Slette gamle containere 15](#_Toc32559998)

# Indledning

OS2nykode er en komponent der gør det muligt at skifte et kodeord i AD via en web-baseret brugergrænseflade.

Anvendelsesmulighederne dækker bl.a.

* Medarbejdere kan skifte deres AD kodeord ved at logge ind med det gamle kodeord, og vælge et nyt (fx til medarbejdere der ikke har en domæne-PC)
* Medarbejdere kan logge ind med deres private NemID, og skifte deres AD kodeord
* Udvalgte medarbejdere kan logge ind, og skifte kodeord på andre medarbejdere, hvor omfanget af hvilke medarbejdere der kan skifte for hvem, styres vha AD grupper

Specielt for skole-området er der funktionalitet til elever, som gør det muligt for forælre at logge ind med deres private NemID, og skifte kodeord på deres børn.

For skole-området er det også muligt at logge ind med sit Uni-login, og skifte ens AD kode.

Endeligt kan OS2nykode konfigureres til at sende SMS’er til brugerne, når deres kodeord skiftes, så de adviseres om ændringen (fx hvis en anden skifter deres kodeord)

# Forudsætninger

OS2nykode er gjort tilgængelig som en Docker komponent, og kan dermed afvikles på både Linux og Windows servere, så længe disse kan afvikle Linux Docker Containere.

Dette er muligt på langt de fleste Linux servere, samt på Windows Server 2019 og nyere.

Følgende skal være til stede før man kan opsætte OS2nykode

* Et virksomhedscertifikat, der er knyttet til en tjensteudbyderaftale hos Nets om brugen af NemID til login, samt en aftale om at bruge PID2CPR tjenesten.
  + Læs evt mere her: <https://www.nets.eu/dk-da/l%C3%B8sninger/nemid/nemid-tjenesteudbyder>
* En aftale om brugen af Familie-servicen på Serviceplatformen (kun hvis forældre skal kunne skifte kodeord på ders børn)
  + Læs evt mere her: <https://www.serviceplatformen.dk/administration/serviceOverview/show?uuid=2419e94b-1760-4fc5-935c-2419ac956e79>
* En aftale om brug af Computopics SMS gateway (hvis man ønsker at sende SMS adviseringer)
  + Læs evt mere her: <https://www.computopic.dk/products/sms-gateway>
* En MySQL kompatibel database hvor OS2nykode kan gemme sin auditlog. Hvis man ikke har en MySQL database, kan man anvende Docker til formålet
* En tilslutning til UniLogin hvis man ønsker at brugere skal kunne logge ind med deres UniLogin for at skifte dere AD brugernavn/kodeord
  + Læs evt mere her: <https://viden.stil.dk/display/INFRA2/Kom+i+gang+med+UNI-Login>

Der er lidt flere oplysninger om disse forudsætninger i underkapitlerne nedenunder. Hvis man allerede har disse tilgængelige, kan man springe til næste kapitel.

## Docker

Docker på Linux er typisk blot at sikre at docker er installeret, enten via apt-get, yum eller lignende installationsværktøj.

Docker på Windows kan installeres som en såkaldt Windows Feature, hvor man tilgår Server Management, og så enabler den Windows Feature der hedder ”Containers”.

Når man har installeret featuren, kan man afvikle såkaldte Windows Containere. Da OS2nykode distribueres som en Linux Container, skal man have konfigureret Docker til at afvikle Linux Containere.

Man kan med fordel tage et kig på denne artikel for hvordan man konfigurerer Windows til dette.

<https://bcthomas.com/2019/02/getting-started-with-linux-containers-on-windows-server-2019/>

Hvis man googler lidt, kan man finde en del artikler om hvordan man anvender Linux Containers på Windows servers (typisk kaldet LCOW, Linux Containers on Windows). Her er det værd at bemærke at man også kan afvikle Linux Containers på Windows 10, men dette gøres på en anden måde end man ville gøre det på en server, så sørg for at der er tale om vejledninger til Windows Server, og ikke Windows 10.

Bemærk også at Hyper-V understøttelse på Windows Serveren er nødvendig, så hvis ens Windows Server er virtualiseret, så skal Hyper-V være slået til, for at der kan afvikles Docker på Windows Serveren.

## NemID tjensteudbyderaftale

For at anvende NemID som en login mekanisme til OS2nykode, skal der være indgået en aftale om brug af NemID med Nets. Teknisk består aftalen af et aftaleid og et virksomhedscertifikatet, og disse skal anvendes under konfigurationen af OS2nykode.

Det er gratis for myndigheder at anvende NemID, men man skal dog stadig indgå en aftale med Nets om brugen af NemID, og gå gennem den samme procedure som alle andre.

Hvis man anvender linket fra oversigten, og foretager en bestilling, er det vigtigt at man husker at bede om adgang til PID2CPR tjenesten, som skal bruges til at lave CPR nummer opslag. Her skal man angive at man er en myndighed, og vil have fuld adgang til servicen.

## Familie servicen

Familieservicen på Serviceplatformen kan anvendes til at finde forældre/værge-relationer, og anvendes af OS2nykode til at understøtte ”forældre kan skifte kodeord på børn”-featuren som er relevant for skole-området.

Man indgår en sådan serviceaftale på samme måde som alle andre serviceaftale på Serviceplatformen, og man kan finde flere oplysninger om dette her

<https://serviceplatformen.dk/>

## SMS Gateway

OS2nykode kan afsende SMS adviseringer ved kodeordsskifte. OS2nykode er gjort klar til at understøtte mange forskellige SMS Gateways, men på nuværende tidspunkt er der konkret udnerstøttelse for Computopics SMS Gateway. Hvis man ønsker understøttelse for andre gateways, kan man tage kontakt til Digital Identity, der gerne bygger yderligere integrationer ind i løsningen.

I Computopics administrationsmodul til SMS Gatewayen kan man oprette brugernavne og kodeord, der kan anvendes til at sende SMS’er. Der skal laves en til OS2nykode, så denne kan afsende SMS’er.

Det er ikke en forudæstning for at bruge OS2nykode løsningen at man har en SMS gateway.

## MySQL

OS2nykode gemmer en auditlog med alle kodeords-skifte, og viser denne log inde i løsningen når en bruger logger ind (så de kan se alle kodeordsskifte der er foretaget på dem).

Man kan enten pege på en eksisterende MySQL database, eller man kan bruge Docker til at starte en lokal MySQL op til formålet.

Andre MySQL kompatible databser som MariaDB og Aurora er også understøttet.

## UniLogin

På skole-området kan det (i det mindste i en kort periode, indtil Uni-Login er udfaset), give mening at anvende Uni-Login som en mekanisme til at skifte det lokale AD kodeord.

Dette forudsætter at man opsætter OS2nykode som en tjenesteudbyder hos STIL på deres uni-login føderation.

Når man gør det, får man brug for SAML metadata fra OS2nykode, som skal leveres til STIL. Disse kan trækkes ud af OS2nykode på endpointet

/saml/metadata

Så hvis man fx har idriftsat OS2nykode på <https://skiftkode.kommune.dk>, så kan man hente metadata filen her

<https://skiftkode.kommune.dk/saml/metadata>

Der er allerede opsat den fornødne integration til UniLogin inde i OS2nykode, men den vil først virke når STIL har registreret ovenstående i deres ende.

## AD (AD FS) login til OS2nykode

En almindelige use-case i OS2nykode, er at man kan logge ind med sit eksisterende brugernavn/kodeord, og så vælge et nyt kodeord.

For at det fungerer, skal man opsætte OS2nykode som en Relying Party i ens lokale AD FS, hvilket gøres ved at hente OS2nykode’s SAML metadata her

/saml/metadata

Så hvis man fx har idriftsat OS2nykode på <https://skiftkode.kommune.dk>, så kan man hente metadata filen her

<https://skiftkode.kommune.dk/saml/metadata>

Disse skal opsættes i kommunens AD FS, hvor man skal udstede et simpel identitets claim. Dvs at den eneste claim rule der skal opsættes i AD FS’en, er en der mapper ”sAMAccountName” til ”Name ID”.

# Konfiguration

OS2nykode er tilgængelig som et Docker image, der ligger på dockerhub til fri afbenyttelse. Besøg nedenstående side for at finde den nyeste udgave af OS2nykode

<https://hub.docker.com/u/os2nykode>

Bemærk at løsningen består af 3 forskellige docker images, og man kun behøves at anvende de docker images der matcher ens behov. Fx er det ikke nødvendigt at anvende os2nykode/sms imaget hvis man ikke skal sende SMS’er fra løsningen.

Man kan anvende Docker på mange forskellige måde, og der er mange værktøje til at starte containere med. Fælles for dem alle er at konfigurationen til et givent image sendes som såkaldte miljø-parametre, der anvendes af docker containeren.

I nedenstående eksempler anvendes Docker Compose til at vise hvordan man konfigurerer OS2nykode, da det er en af de simpleste modeller. Hvis man anvender andre teknologier (fx Kubernetes), skal man anvende de samme miljø-parameter, på hvad end måde de sættes op i ens valgte Docker værktøj.

## Miljø-parametre

Nedenfor er beskrevet de parametre som man kan bruge til at styre OS2nykode. Parametrene er indelt i afsnit der matcher de docker images som indgår i den samlede løsning.

### Miljø parametre for SMS modulet

For at integrere til SMS modulet, skal man have opsat et brugernavn og kodeord til formålet i Computopics SMS gateway. Dette styrer hvad der står som afsender på den SMS’er som sendes fra løsningen.

De miljøparametre der skal opsættes er følgende

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Eksempel** | **Beskrivelse** |
| type | Computopic | Angiver hvilken SMS gateway der anvendes. Pt er der kun understøttet én SMS gateway ”Computopic”. |
| username | KommuneIT | Brugernavnet til SMS gatewayen |
| password | 1234 | Det kodeord som er opsat i SMS gatewayen til afsendelse af SMS’er |

### Miljø parametre for Familie modulet

Familiemodulet forudsætter at man har indgået en aftale om brug af Familie servicen (en såkaldt Serviceaftale). Denne aftale kan findes inde i KOMBITs Administrationsmodul, og her kan man finde de parametre der er nødvendige

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Eksempel** | **Beskrivelse** |
| OmFamilieService:certPath | /home/cert/keystore.pfx | Angiver stien til den P12/PFX fil som indeholder certifikatet der skal kalde Serviceplatformen servicen. |
| OmFamilieService:certPassword | Kodeord1234 | Kodeordet til ovenstående P12/PFX fil. |
| ServiceAgreement:uuid | 818ba401-07d1-4c9d-b8d8-b2d30cef915f | UUID’et på den Serviceaftale der er indgået. Man kan aflæse UUID’et i KOMBITs Administrationsmodulet når man ”viser” serviceaftalen. |
| ServiceAgreement:userUuid | 67d6f575-4669-4092-953c-4f06688c633d | UUID’et på ens egen kommune. Hver kommune har et unikt UUID, og disse kan findes på KOMBITs sharepoint site (eller ved at kontakte Serviceplatformens helpdesk) |
| ServiceAgreement:systemUuid | 9ebc1f2f-c316-498b-b23f-12adf10ebd1b | UUID’et på det it-system der skal kalde Familie servicen (kan findes inde i KOMBITs administrationsmodul, når man ”viser” it-systemet) |

Da familie modulet skal bruge et certifikat, er det nødvendigt at mounte et volume i Docker, der peger på en folder der indeholder P12/PFX filen. I eksempel sidst i dette kapitel, kan man se hvordan man mounter et volume vha Docker Compose.

### Miljø parametre for OS2nykode grundmodulet

OS2nykode modulet har langt de fleste konfigurationsparametre, og de er beskrevet i detaljer nedenfor. Bemærk at ikke alle parametre behøves være udfyldt, og I så fald skal man blot sætte dem til en tom streng som værdi (fx: ””).

Da der er mange parametre, er de grupperet nedenfor, med tomme rækker mellem de enkelte afsnit, så man kan se hvad der hænger sammen.

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Eksempel** | **Beskrivelse** |
| spring.datasource.driver-class-name | com.mysql.cj.jdbc.Driver | Hvilken SQL driver skal bruges til at forbinde til databasen. |
| spring.datasource.url | jdbc:mysql://mysql/os2nykode | En SQL connection string, der peger på den MySQL database hvor auditloggen skal opbevares |
| spring.datasource.username | os2nykode | Brugernavnet til SQL databasen |
| spring.datasource.password | HemmeligtKodeord | Kodeordet til SQL databasen |
|  |  |  |
| ldap.url | ldaps://dc1.kommune.dk | En forbindelsesstreng til en domain controller. Bemærk at forbindelsen SKAL ske over LDAPS (krypteret LDAP), ellers er kodeordsskifte ikke muligt. |
| ldap.base | dc=kommune,dc=dk | Et DN der peger på det område i AD hvor OS2nykode må lede efter brugere og grupper. Typisk sættes dette til roden af AD’et. |
| ldap.username | admin@kommune.dk | UPN på en brugerkonto der må udføre password skifte. |
| ldap.password | SuperHemmeligeKode | Passwordet på ovenstående brugerkonto |
| ldap.cert.trustall | true | Typisk er det SSL certifikat der ligger på en domain controller et selv-udstedt certifikat, som omverdenen ikke stoler på, så man skal formodentligt sætte denne værdi til ”true” for at forbindelsen kan etableres. |
| ldap.field.ssn | employeeID | En pegepind til den attribut i AD, hvor brugernes personnummer står.  Hvis dette felt er markeret som værende følsomt, så skal ovenstående brugerkonto have adgang til at læse følsomme attributter. |
|  |  |  |
| ldap.groups.cannotChangePwd | cn=IngenKodeordsSkifte, dc=kommune,dc=dk | DN på en gruppe i AD, hvor medlemmerne deraf aldrig må skifte kodeord via OS2nykode.  Kan være tom. |
| ldap.groups.pwdCirclesOU | ou=PasswordGrupper | En pegepind til en OU i AD, hvor alle password grupperne ligger (se mere nedenfor). Værdien er relativ til ldap.base |
| ldap.groups.canChangeOthersPwd | cn=CanChangePwd, dc=kommune, dc=dk | DN på en bestemt gruppe i AD som man skal være medlem af, for at måtte skifte kodeord på andre. |
| ldap.groups.cannotBeChangedPwdOn | cn=CannotBeChangedPwdOn, dc=kommune, dc=dk | DN på en gruppe hvor brugerne deri aldrig kan få skiftet kodeord af andre via OS2nykode |
| ldap.groups.masterPwdAdmins | cn=MasterAdmins, dc=kommune, dc=dk | DN på en gruppe af super administratorer, der godt må skifte kodeord på medlemmerne af canChangeOthersPwd gruppen |
|  |  |  |
| omfamilie.url | http://omfamilie:5000  /api/CPRLookup | URL endpoint på familie servicen (docker containeren der udstiller servicen).  Kan være tom. |
|  |  |  |
| sms.gateway.url | http://smsgateway:5000/ | URL endpoint på SMS servicen (docker containeren der udstiller servicen).  Kan være tom. |
| ldap.field.mobile | mobile | Den attribut i AD hvor brugernes mobilnummer står. Hvis attributten ikke er udfyldt, eller en given bruger ikke har noget nummer, så sendes blot ikke nogen SMS |
| sms.message | Dit kodeord er skiftet | Den besked der sendes på SMS’en til brugeren. |
|  |  |  |
| Login.enable.nemid | true | Hvis brugerne skal kunne logge ind med NemID, så skal denne sættes til ”true” |
| Login.enable.unilogin | false | Hvis brugerne skal kunne logge ind med deres Uni Login, så skal denne sættes til ”true” |
| Login.enable.idp | true | Hvis brugerne skal kunne logge ind med deres AD brugernavn/kodeord, så skal denne sættes til true |
|  |  |  |
| saml.baseUrl | https://kode.kommune.dk | Hvis man har slået idp eller unilogin til i ovenstående, så skal denne udfyldes med det URL endpoint som OS2nykode kan tilgås på |
| saml.keystore.location | file:config/keystore.pfx | Navn på det certifikat der skal bruges til SAML opsætningen (til ovenstående) |
| saml.keystore.password | KodeordTilPfx | Kodeord til certifikatet |
| saml.metadata.idp.url | https://adfs.kommune.dk/  FederationMetadata/2007-06/FederationMetadata.xml | Endpoint til kommunens AD FS (eller anden IdP) metadata fil |
| saml.metadata.idp.entityid | http://adfs.kommune.dk/  adfs/services/trust | Navn på IdP’en (kan læses i metadata filen) |
|  |  |  |
| password.defaultPolicy.minLength | 4 | Minimumlænge på brugerens nye kodeord |
| password.defaultPolicy.maxLength | 64 | Maxlænge på brugerens nye kodeord |
| password.defaultPolicy.  upperAndLowerCaseRequired | true | Hvorvidt brugeren skal vælge både store og små bogstaver i sit kodeord |
| password.defaultPolicy.  specialCharactersRequired | false | Hvorvidt specialtegn er krævet |
| password.defaultPolicy.  lettersRequired | true | Hvorvidt bogstaver er krævet |
| password.defaultPolicy.  digitsRequired | false | Hvorvidt tal er krævet |
|  |  |  |
| password.policies[i].groupName | cn=politik1,ou=politikker,  dc=kommune,dc=dk | DN på en AD grupper, der repræsenterer denne password politik |
| password.policies[i].minLength | 4 | Minimumlænge på brugerens nye kodeord |
| password.policies[i].maxLength | 64 | Maxlænge på brugerens nye kodeord |
| password.policies[i].  upperAndLowerCaseRequired | true | Hvorvidt brugeren skal vælge både store og små bogstaver i sit kodeord |
| password.policies[i].  specialCharactersRequired | false | Hvorvidt specialtegn er krævet |
| password.policies[i].  lettersRequired | true | Hvorvidt bogstaver er krævet |
| password.policies[i].  digitsRequired | false | Hvorvidt tal er krævet |

Da OS2nykode docker containeren også har brug for adgang til keystores, og NemID konfigurationsfiler, skal der mountes et volume, hvor disse filer er tilgængelige. I eksemplet nedenfor er vist hvordan man gør dette med Docker Compose.

Nogle af ovenstående konfigurationer kræver lidt mere forklaring, og er beskrevet i underkapitlerne herunder.

Det volume der mountes, skal (hvis man bruger NemID integrationen) indeholde 2 konfigurationsfiler til NemID. Disse skal have følgende navne, og indeholde følgende oplysninger

**Fil:**

nemid.properties

**Indhold:**

oces2.environment=OCESII\_DANID\_ENV\_PROD

nemid.applet.server.url.prefix=https://applet.danid.dk

nemid.serviceprovider.logonto=XXXX

nemid.applet.parameter.signing.keystore=classpath:XXXX.pfx

nemid.applet.parameter.signing.keystore.password=XXXX

I forbindelse med at man har indgået en tjenesteudbyderaftale med Nets om brug af NemID, har man fået en mail fra Nets, hvor navnet på ens aftale indgår, ”logonto” delen af ovenstående skal indeholde dette navn, og det virksomhedscertifikat man skal anvende til aftalen skal ligge i samme folder, og navn på certifikatfilen, samt kodeord til certifikatfilen skal stå i konfigurationsfilen.

**Fil:**

pid.properties

**Indhold:**

pid.url=https://pidws.certifikat.dk/pid\_serviceprovider\_server/pidxml/

pid.serviceproviderid=XXXX

pid.keystore.location=classpath:XXXX.pfx

pid.keystore.password=XXXX

Det samme certifikat som anvendes til NemID skal anvendes til PID2CPR opslaget, og de samme værdier skal indtastes her. I samme mail fra Nets, hvor man har fået aftalen med NemID, er der også aftaleoplysninger på PID2CPR tjenesten, hvor man har fået et såkaldt SPID (typisk 9 cifre). Dette skal indtastes som serviceproviderid i ovenstående fil.

## Password politikker

Når man konfigurerer OS2nykode, kan man opsætte password politikker som brugerens nye kodeord skal overholde. Det er krævet at der er udfyldt en default politik, og man kan tilføje ekstra optionelle password politikker som styres via AD grupper.

Alle ekstra politikker skal pege på en gruppe i AD, og der gælder den regel, at hvis en bruger er medlem af en password politik gruppe, så gælder denne password politik for brugeren, og hvis en bruger ikke er medlem af en sådan gruppe, så gælder default politikken for brugeren.

Password politikker nummeres i konfigurationsfilen, og i tabellen ovenfor står der [i] i parameternavnet, her skal stå [0], [1], [2], osv for de politikker man opretter. Se evt eksemplet i næste kapital.

# Eksempel Docker Compose fil

Nedenfor er en fuldt valid Docker Compose konfigurationsfil, der også indeholder en docker-styret MySQL database til at holde auditloggen.

version: "2.1"

services:

mysql:

image: mysql:5.6

restart: always

environment:

MYSQL\_RANDOM\_ROOT\_PASSWORD: "yes"

MYSQL\_PASSWORD: "Test1234"

MYSQL\_USER: "os2nykode"

MYSQL\_DATABASE: "os2nykode"

volumes:

- ./db:/var/lib/mysql

smsgateway:

image: os2nykode/sms:2020-01-16

restart: always

environment:

type: "Computopic"

username: "KommuneIT"

password: "1234"

omfamilie:

image: os2nykode/familie:2020-01-16

restart: always

environment:

OmFamilieService:certPath: "/home/cert/Serviceplatformen.pfx"

OmFamilieService:certPassword: "Test1234"

ServiceAgreement:uuid: "07bbff01-e309-4853-ae80-851a9c2cab55"

ServiceAgreement:userUuid: "a689fe9f-abe0-48bd-a34e-a727690a4647"

ServiceAgreement:systemUuid: "dc2b43e2-1916-423a-a02d-1694705ec2d5"

volumes:

- ./config:/home/cert

os2nykode:

image: os2nykode/os2nykode:2020-02-28

restart: always

ports:

- 9500:9500

environment:

spring.datasource.driver-class-name: "com.mysql.cj.jdbc.Driver"

spring.datasource.url: "jdbc:mysql://mysql/os2nykode"

spring.datasource.username: "os2nykode"

spring.datasource.password: "Test1234"

ldap.url: "ldaps://dc01.kommune.dk"

ldap.base: "dc=kommune,dc=dk "

ldap.username: "pwdadmin@kommune"

ldap.password: "Test1234"

ldap.cert.trustall: "true"

ldap.field.ssn: "employeeID"

ldap.groups.pwdCirclesOU: "ou=pwdgrupper,dc=commune,dc=dk"

ldap.groups.cannotChangePwd: "cn=NoChangePwd,ou=grupper,dc=kommune,dc=dk"

ldap.groups.cannotBeChangedPwdOn: "CN=PwdDisabled,ou=grupper,dc=kommune,DC=dk"

ldap.groups.canChangeOthersPwd: "cn=PwdAdmins,ou=grupper,dc=kommune,dc=dk"

ldap.groups.masterPwdAdmins: "cn=PwdMasterAdmins,ou=grupper.dc=kommune,dc=dk"

omfamilie.url: "http://omfamilie:5000/api/CPRLookup"

sms.gateway.url: "http://smsgateway:5000/"

sms.message: "Dit kodeord er nu skiftet i AD"

ldap.field.mobile: "mobile"

login.enable.nemid: "true"

login.enable.unilogin: "false"

login.enable.idp: "true"

saml.baseUrl: "https://skiftkode.kommune.dk"

saml.keystore.location: "file:config/keystore.pfx"

saml.keystore.password: "Test1234"

saml.metadata.idp.url: "https://adfs.kommune.dk/FederationMetadata/2007-06/FederationMetadata.xml"

saml.metadata.idp.entityid: "http://adfs.kommune.dk/adfs/services/trust"

password.defaultPolicy.minLength: "4"

password.defaultPolicy.maxLength: "64"

password.defaultPolicy.upperAndLowerCaseRequired: "false"

password.defaultPolicy.specialCharactersRequired: "false"

password.defaultPolicy.lettersRequired: "true"

password.defaultPolicy.digitsRequired: "true"

password.policies[0].groupName: "cn=politik1,ou=groups,dc=kommune,dc=dk"

password.policies[0].minLength: "4"

password.policies[0].maxLength: "8"

password.policies[0].upperAndLowerCaseRequired: "true"

password.policies[0].specialCharactersRequired: "false"

password.policies[0].lettersRequired: "true"

password.policies[0].digitsRequired: "true"

password.policies[1].groupName: " cn=politik2,ou=groups,dc=kommune,dc=dk "

password.policies[1].minLength: "1"

password.policies[1].maxLength: "16"

password.policies[1].upperAndLowerCaseRequired: "false"

password.policies[1].specialCharactersRequired: "false"

password.policies[1].lettersRequired: "false"

password.policies[1].digitsRequired: "false"

password.policies[2].groupName: " cn=politik3,ou=groups,dc=kommune,dc=dk "

password.policies[2].minLength: "1"

password.policies[2].maxLength: "16"

password.policies[2].upperAndLowerCaseRequired: "false"

password.policies[2].specialCharactersRequired: "true"

password.policies[2].lettersRequired: "false"

password.policies[2].digitsRequired: "false"

volumes:

- ./config:/config

# Docker kommandoer

Når man anvender Docker, er der nogle enkelte kommandoer man med fordel kan lære, som kan gøre det nemmere at drifte OS2nykode.

Alle kommandoer afvikles via Powershell, som administrator

## Starte og/eller genstarte applikationen

OS2nykode kommer med en Docker Compose konfigurationsfil (se afsnit 4). Hvis man i powershell står i samme folder som docker-compose.yml filen, kan man starte applikationen op ved at skrive

$ docker-compose.exe up -d

”-d” er vigtig, da det sikrer at applikationen starter op i baggrunden. Hvis man undlader ”-d”, så hænger applikationen i powershell konsollen, og stopper når man lukker konsollen.

Hvis der er ændringer til docker-compose.yml konfigurationsfilen, så vil ovenstående kommando også kunne anvendes til at genstarte de containere som har ændringer.

## Se alle kørende containere

Når applikationen kører, og man ønsker at se status på disse, så kan man bruge nedenstående kommando til at liste alle kørende containere på serveren

$ docker ps

I output kan man se hvilke containere der kører, hvor langt tid de har været kørende, hvilke porte de lytter på, og nok mest vigtigt, man kan se PID’en på den enkelte container (længest til venstre står PID’en).

## Se loggen fra en container

Hvis man ønsker at kigge i loggen fra en bestemt container, så skal man først finde PID’en på den container hvis log man ønsker at kigge i (se ovenfor). Når man har den, så kan man anvende følgende kommando i powershell til at kigge i loggen

$ docker logs -f PID

Hvor PID erstattes med den faktiske værdi for den valgte container.

Man kan undlade ”-f” parametren. Den sikrer blot at logfilen holdes åben, og evt ændringer til logfilen automatisk skrives ud i konsollen (CTRL+C for at lukke logfilen igen).

## Stoppe en container

Hvis man har en container man ønsker at stoppe, så skal man også bruge PID’en. Når man har den, kan man anvende følgende kommando til at stoppe containeren

$ docker stop PID

Bemærk at Windows er notorisk langsom til at stoppe containere, og hvis det haster, kan man tvinge en nedlukning øjeblikkeligt, ved at skrive

$ docker kill -s 9 PID

OS2nykode har det ok med at blive lukket på den måde, men ikke alle containere håndterer det lige godt (fx bør man ikke lukke database containeren på denne måde).

## Slette gamle containere

Docker sletter som udgangspunkt ikke nogen containere, så over tid kan man opleve at Docker anvender mere og mere diskplads. Fx når man opdaterer OS2nykode, så vil både den gamle og nye version være på serveren.

For at slette alle gamle containere, kan man anvende denne kommando

$ docker system prune -a