OS2MO opsætning

Viborg Kommune OS2MO Server og Powershell remote server opsætning.

OS2MO Server

OS2MO Serveren ved Viborg Kommune er en Ubuntu 16.04 (men forhør jer ved Magenta inden opsætning da OS version krav / anbefaling kan ændre sig)

Ubuntu Serveren har vi opsat så den er Domain Joined og vores serverfolk og eksterne Magenta konsulenter dermed kan bruge AD Brugernavn og kode til at logge på serveren. Rettigheder styres derved via AD, som tilfældet er med Windows servere.

Trin for at lave Ubuntu Serveren: (Husk at gennemgå og rette scriptet da der er spor efter den opsætning vi har i Viborg Kommune)

- Installer Ubuntu serveren via ISO (det anbefales at man har som minimum bruger kendskab til Linux og SSH for at udføre denne guide)
    - Under installationen skal der opsættes Fast IP på serveren.

1. Opsæt Hosts fil, opsætning af ubuntu pakker biblioteker (APT) samt installer alle nødvendige pakker til Domain Join.

Alle kommandoer er kørt som super user på systemet. (sudo -i)

#Part 1 : Indsæt Hostname i /etc/hosts filen

hostname=$(hostname -s) # we use this variable to make life easier

echo "127.0.0.1 $hostname.viborg.local $hostname" >> /etc/hosts

Se om DNS er opsat korrekt.

systemd-resolve --status

#Part 2 : Opdater pakke biblioteker og installer pakker.

bruger sed til at erstatte 'main' med 'main restricted universe'

sed -i 's/main/main restricted universe/g' /etc/apt/sources.list

apt update

installer pakkerne

apt install realmd sssd sssd-tools samba-common krb5-user packagekit samba-common-bin samba-libs adcli ntp ntpdate -y

2. #### Vi har ved Viborg Kommune valgt at disable IPv6 fra alle servere da vi har oplevet problemer med at tilgå servere fra visse lokationer grundet routing. ####
   #### Snak med jeres interne netværk team om dette også er noget i bør gøre i jeres opsætning ####

#Part 3 : Deaktivering af IPv6

#alle kommandoer skal afvikles med root privileger

echo "net.ipv6.conf.all.disable_ipv6 = 1" >> /etc/sysctl.d/99-sysctl.conf

echo "net.ipv6.conf.default.disable_ipv6 = 1" >> /etc/sysctl.d/99-sysctl.conf

echo "net.ipv6.conf.lo.disable_ipv6 = 1" >> /etc/sysctl.d/99-sysctl.conf

#genlæs sysctl konfiguration

sysctl -p

3. Opsætning af NTP-synkronisering af tid samt opsætning af konfiguration til realmd

#Part 4 : Opsæt timezone og npt client – "viborg.local" anvendes som ntp server i Viborg, da det er et DNS navn, som returnerer ip på vores 3 domæne controller servere, som har NTP service kørende.

timedatectl set-timezone Europe/Copenhagen

#First we insert out npt server in the list

sed -i '/# Specify one or more NTP servers./a \server viborg.local' /etc/ntp.conf

#Then we mask the ubuntu pool from the list, we use regexp to find 'pool *.ubuntu' and replace it with a masked version.

sed -i -r 's/pool (.*).ubuntu/#pool \1.ubuntu/g' /etc/ntp.conf

systemctl restart ntp

Husk at rette jeres domain navne og os-version så den passer til jeres miljø.

Det vi opsættter i realmd.conf er hvor vi ønsker at bruger "home" biblioteker skal placeres samt nødvendige domæne oplysninger og specificering af AD klient type.

Yderligere info kan findes på
http://manpages.ubuntu.com/manpages/bionic/man5/realmd.conf.5.html

#Part 5 : Opsæt realmd

cat <<EOT > /etc/realmd.conf

[users]

default-home = /home/%D/%U

default-shell = /bin/bash

[active-directory]

default-client = sssd

os-name = Ubuntu Server

os-version = 16.04

[service]

automatic-install = no

[viborg.local]

fully-qualified-names = no

automatic-id-mapping = yes

user-principal = yes

manage-system = no

EOT

4. Efter opsætningen af Realmd udføres selve Domain Join, brugeren vi benytter til kommandoerne her under skal have lov til at melde computeren (OS2MO serveren) ind i domænet.

DETTE SKAL KØRES MANUELT EN LINJE AF GANGEN

#Part 6 : Initier Kinit og der efter meld ind i domainet. # Dette step skal køres en kommando af gangen da den ellers ikke vil virke.

kinit admnils@viborg.local

Vi bør nu have modtaget et kerberos ticket fra vores AD til vores Domain bruger. Vi kan hvis vi ønsker at verificere dette køre kommandoen herunder.

klist

Start - output fra succesfuld klist kommando

Ticket cache: FILE:/tmp/krb5cc_790070301_wj44Ws

Default principal: admnils@VIBORG.LOCAL

Valid starting Expires Service principal

05/03/2019 13:02:39 05/03/2019 23:02:39 krbtgt/VIBORG.LOCAL@VIBORG.LOCAL

renew until 05/04/2019 13:02:39

Slut - output fra succesfuld klist kommando

Med et kerberos ticket på maskinen kan vi foretage domain join.

realm --verbose join -U admnils viborg.local

#Læg her mærke til at der er skrevet Brugernavn “mellemrum” domæne.

5. Vi strammer nu sikkerheden så det kun er Domain Admins og en bestemt gruppe der kan tilgå serveren. Opret en AD gruppen som du ønsker at bruge til at styre hvilke AD konti der skal have

Administrator rettigheder til OS2MO serverne. I Viborg har vi kaldt gruppen:
”SVR_OS2MO_OS2MOPROD.viborg.local_Administrators”

#Part 7 : Opsæt Realm til kun at tillade login af Domain Admins

realm deny --all

realm permit -g 'Domain Admins' 'SRV_OS2MO_(indsæt servernavn)_Administrators'

systemctl restart sssd

6. Opsætter Home mappe på linux serveren samt opsætter Samba.
   Samba skal kun bruges hvis man ønsker at kunne tilgå mapper på et Windows File Share.

#Part 8 : Opsæt automatisk opsætning af Homedir

sed -i -e '/pam_sss.so/a \#Inserted by Script - NIR\nsession required pam_mkhomedir.so skel=/etc/skel/ umask=0077\n#End Inserted by Script - NIR' /etc/pam.d/common-session

#Part 9 : Opsæt Samba

cp /etc/samba/smb.conf /etc/samba/smb.conf.initial #Backup intial config

sed -i '/\[global\]/a workgroup = VIBORG\nclient signing = yes\nclient use spnego = yes\nkerberos method = secrets and keytab\nrealm = VIBORG.LOCAL\nsecurity = ads' /etc/samba/smb.conf

7. Og sikrer os at de grupper vi ønsker har adgang til at køre kommandoer som super user.

#Part 10 : Opsæt Sudoers filen

cat <<EOT >> /etc/sudoers.d/domainusers

Allow domain users to use the sudo command
%domain\ admins ALL=(ALL:ALL) ALL
%SRV_OS2MO_(indsæt servernavn)_Administrators ALL=(ALL:ALL) ALL
EOT
chmod 0440 /etc/sudoers.d/domainusers

#Part 11 : Opdater maskinen og Genstart

apt upgrade -y && reboot

Nu kan vi logge på maskinen med vores AD-brugernavn, og styring af rettighederne foregår i vores AD.

En bruger i AD gruppen ’SRV_OS2MO_(indsæt servernavn)_Administrators’ vil automatisk på Login rettigheder og mulighed for at elevere til super user på serveren.

Management Server til afvikling af Powershell fra OS2MO

Vi har ved Viborg Kommune, ud over OS2MO Serverene, opsat en Management server der afvikler alle remote scripts til eks. AD, Office 365 eller andre dele der skal kunne hentes data fra eller sendes data til fra OS2MO systemet.

Serveren vi benytter til dette, er en Windows Server 2016 Standard med Remote Administration værktøjer til bl.a. AD.
Serveren skal have installeret alle de PowerShell moduler som skal anvendes af OS2MO AD integrationen. Eksempelvis AD modulet, Azure AD moduler mv.

Serveren er opsat så den tillader Remote Management via WMI/WSMAN

Dette gøres nemmest ved at oprette en AD Gruppe med de ønskede brugere eller service konti og tilføje denne gruppe til 'Remote Management Users' gruppen på serveren.

På den måde styrer vi rettighederne i vores AD og giver os en større synlighed over hvem der har hvilke rettigheder.
I Viborg Kommune, har vi oprettet en specifik servicekonto (AD konto), som OS2MO AD integrationen anvender til at eksekvere Powershell. Denne servicekonto er medlem af "Remote Management Users" gruppen på serveren.

Active Directory – beskyttelse af følsomme data (CPR Nummer).

Denne del af guiden er kun tilføjet for at dele hvordan vi har håndteret at have CPR nummer i vores AD, samt hvordan vi har skjult denne attribut for alle andre end de personer og services der skal have lov til at tilgå CPR nummer.

Baggrund: I vores AD har vi valgt at have CPR nummer tilknyttet alle vores brugere, dette bruges til bl.a. password skifte via NemId og til SoloID MFA på vores ADFS-forbindelser.

Da en normalt AD Attribut er synligt for alle var dette ikke en mulighed at lade CPR-nummer attributten forblive synlig.

Vi har derfor ændret CPR-nummer attributten til Confidential

Dette kan vi gøre ved at sætte searchFlags på attributten til 128 (0x80).

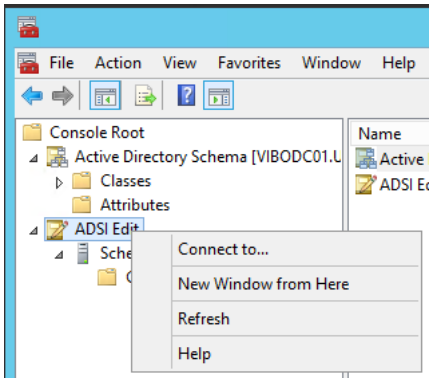
Fremgangsmåde:

Log på en DC server. Dette er påkrævet for at skrive til searchFlags på attrubutes.

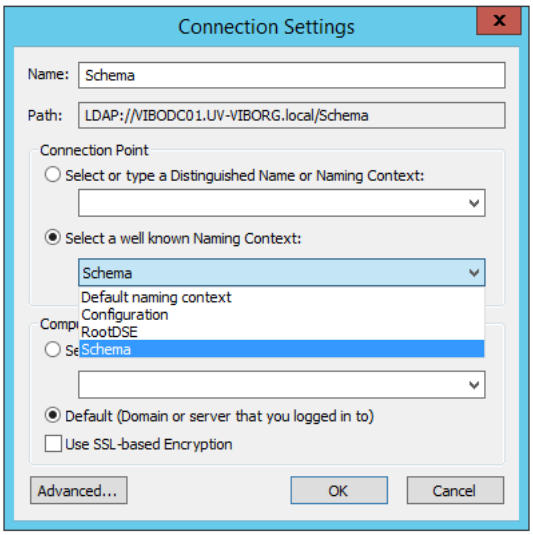
Åben MMC som Administrator

Tilføj ADSI Edit

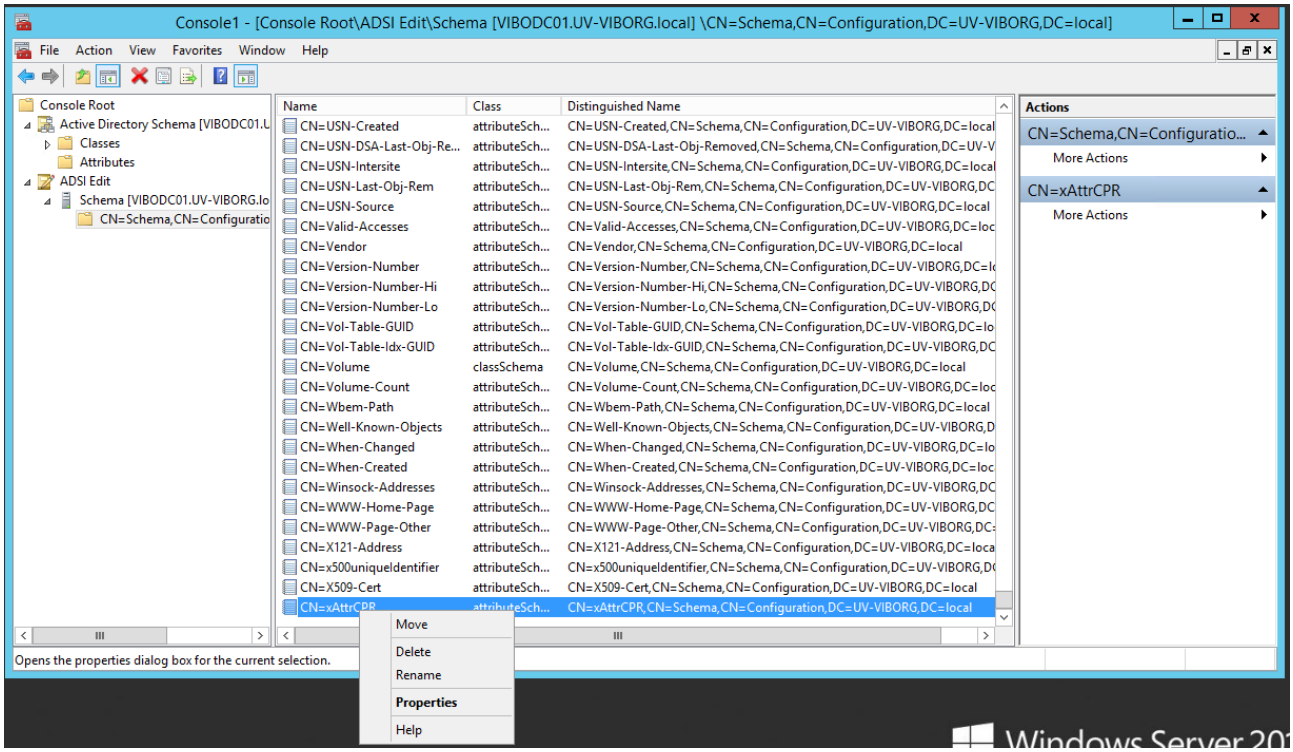
Højreklik på ADSI Edit og vælg "Connect to…"



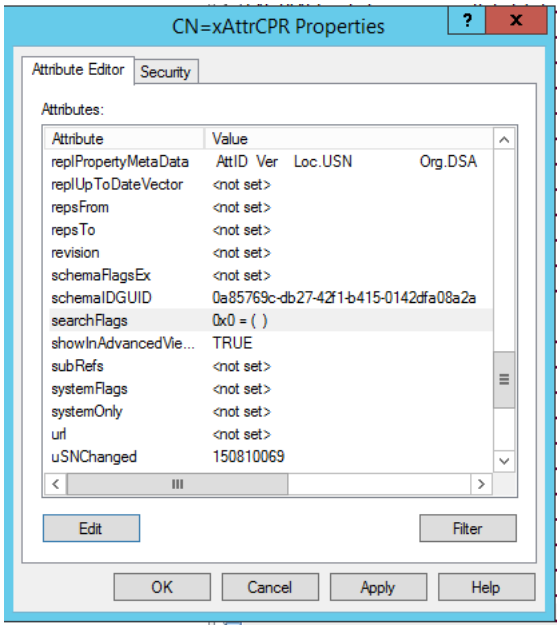
I Select a well known Naming Context: vælges Schema



Find den Attribute du ønsker at ændre, højreklik på den og vælg Properties



I properties find og vælg “searchFlags” og tryk på Edit

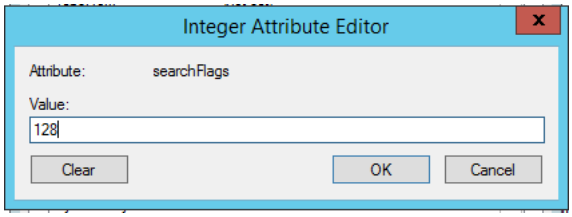


Værdien i searchFlags er en samling af bits 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 hvor det 8. bit = 128 = Confidential flag.

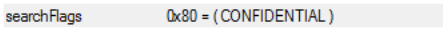
Værdierne kan ses her: https://msdn.microsoft.com/en-us/library/cc220851.aspx

Hvis værdien ikke er 0 skal du kontrollere hvad værdien er og sikre at 128 bit er sat.

Værdien er pr. default 0 eller tom. Sæt den til 128.



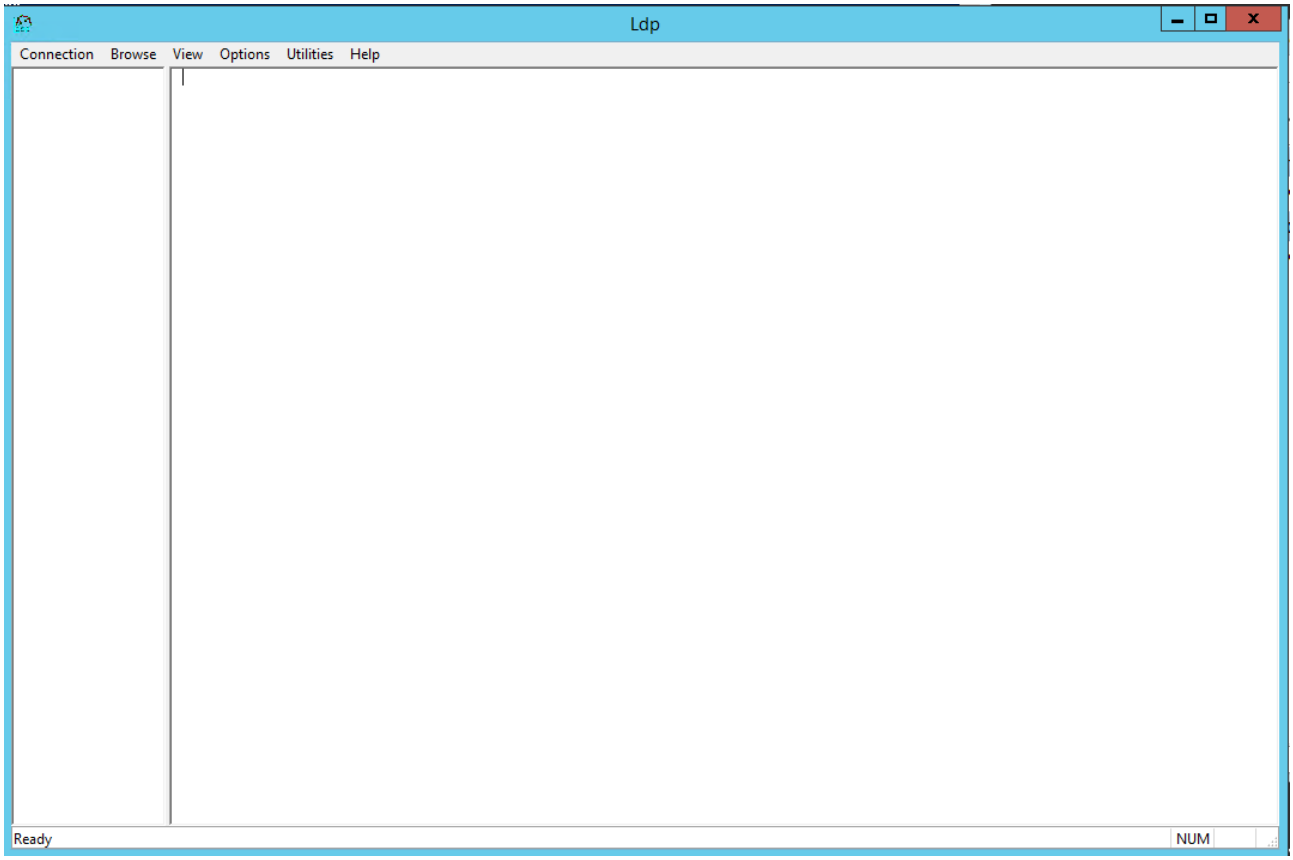
Når den er sat vises følgende I searchFlags feltet



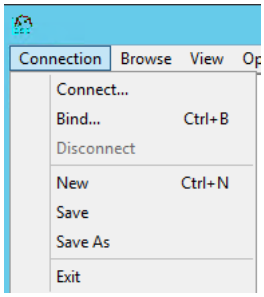
Tryk OK for at gemme opsætningen.

For at sætte adgang til attributten op skal vi ldp.exe bruges.

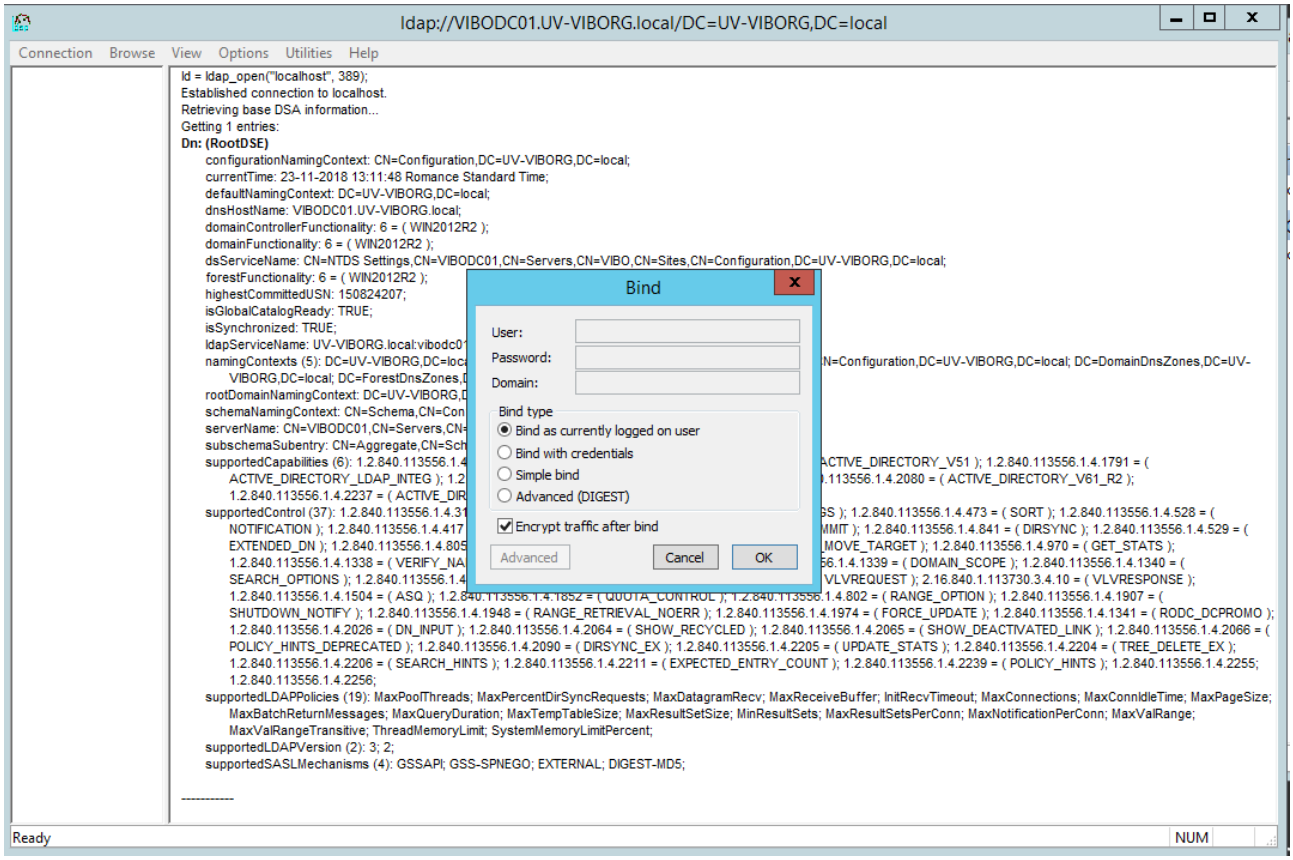
Åben ldp.exe som administrator (dette gøres nemmest ved at åbne en Command Prompt som Administrator og i den åbne ldp.exe)



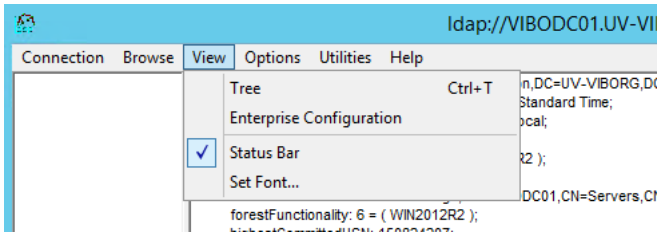
Vælg Connection, og Connect, i Connection dialogen skriv localhost og tryk OK (kun hvis den kører på DC serveren).



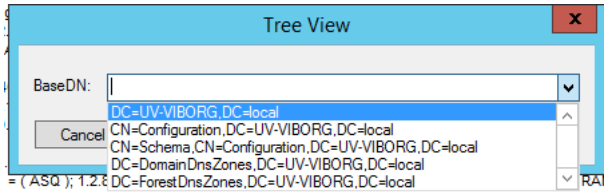
Tryk på Bind og tryk OK



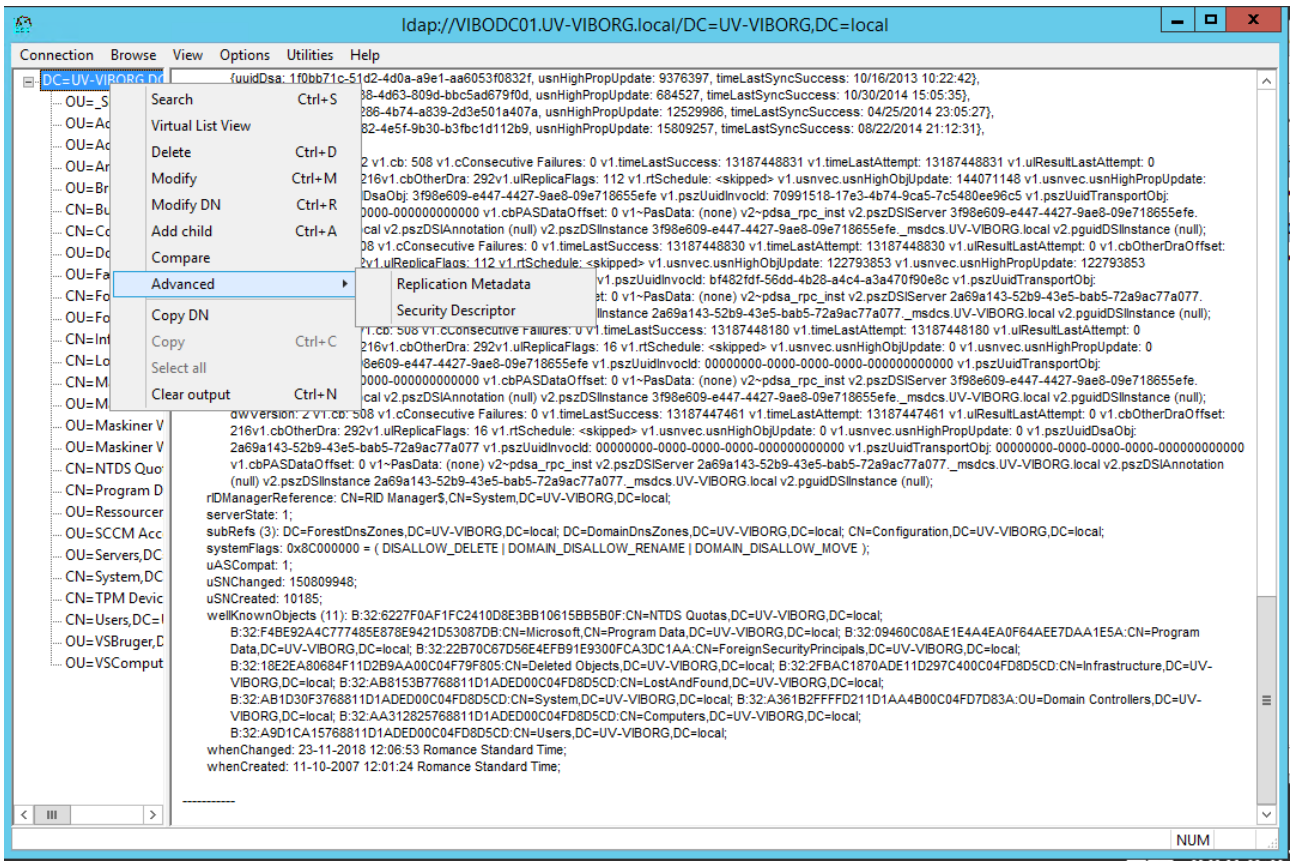
Vælg View og Tree



Vælg DC=UV-VIBORG,DC=local og tryk OK



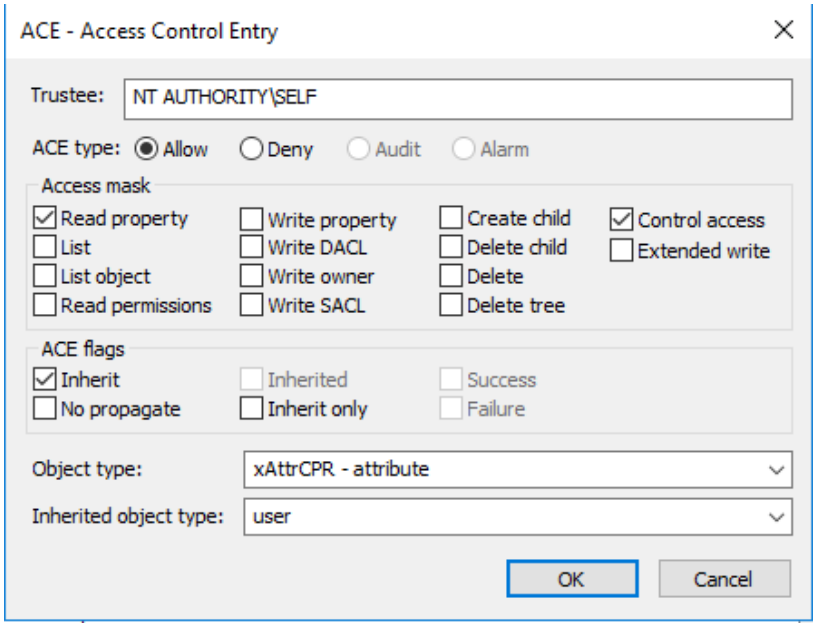
Højreklik på Root elementet, vælg Advanced – Security Descriptor og tryk OK på den pop-up der kommer.



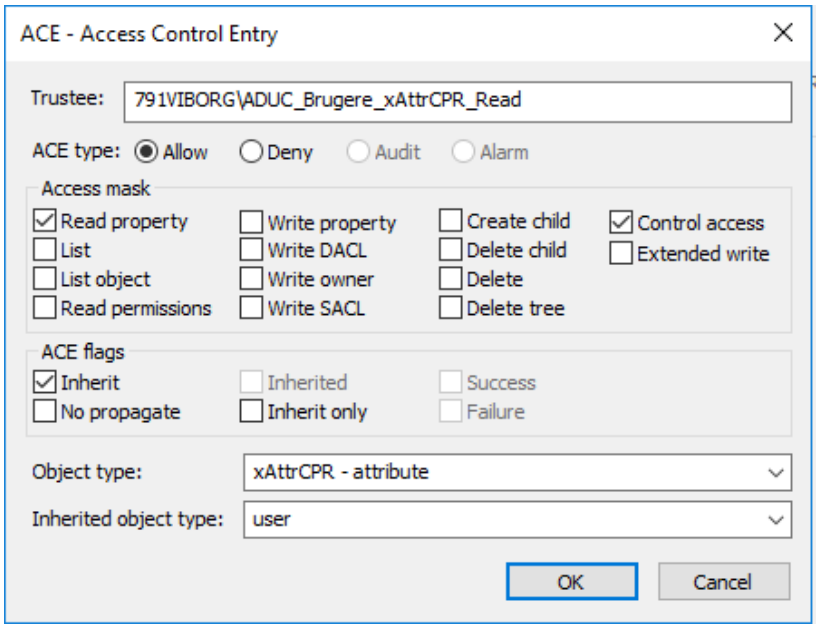
Opret 3 nye ACE med nedenstående oplysninger.

For at tilføje en ACE, vælg en eksisterende ACE i listen og tryk op Add ACE i bunden af vinduet til venstre.

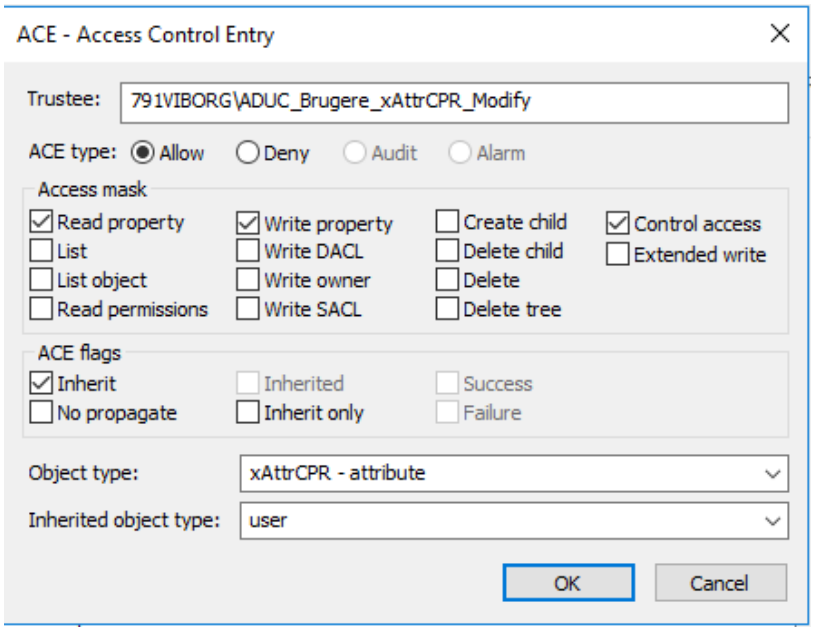
Trustee: NT AUTHORITY\SELF



Trustee: DOMAIN\ADUC_Brugere_xAttrCPR_Read



Trustee: DOMAIN\ADUC_Brugere_xAttrCPR_Modify



Når de ønskede ændringer er lavet i Security Descriptor vinduet trykkes på Update for at gemme opsætningn.

Herefter kan ldp lukkes ned.

Service bruger til afvikling af scripts.

For at kunne sikre vores miljø bedst muligt oprettet vi dedikerede Service brugere til alle services der skal køre i vores server miljø.

OS2MO er ingen undtagelse.

Vi har til OS2MO oprettet SVC_OS2MO_ServiceUser der er blevet tildelt rettigheder til de nødvendige grupper i AD.

Vi tildeler ikke adgang direkte på en bruger, men på grupper som vi så melder brugere ind i.

Vores OS2MO bruger har bl.a. adgang til at logge på OS2MO Management serveren via Remote management, den er Domain User så den har lov til at læse alle ikke skjulte attributter i AD og den er medlem af gruppen der tildeler adgang til at lære og skrive i CPR-nummer attributten.