OS2MO opsætning

OS2MO Server og PowerShell remote server opsætning.

OS2MO Server

OS2MO Serveren er en Ubuntu 20.04 (men kontroller dokumentation eller 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 det er rettet en del til for at anonymisere, der hvor der står 'domain.name' skal jeres fulde domænenavn stå, hvor der blot står 'domain' skal den førte del af domænenavnet stå, hvor der står 'administrator_name' skal jeres domain administrators brugernavn stå)

- 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 \$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 krb5-user packagekit adcli ntp ntpdate -y

 #### Vi har 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 – "domain.name" anvendes som ntp server, da det er et DNS navn, som returnerer ip på 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 domain.name' /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 <u>http://manpages.ubuntu.com/manpages/bionic/man5/realmd.conf.5.html</u>

#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 = 22.04

[service]

automatic-install = no

[domain.name]

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 herunder 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 domænet. # Dette step skal køres en kommando ad gangen da den ellers ikke vil virke.

kinit administrator_name@domain.name

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: administrator_name@DOMAIN.NAME

Valid starting Expires Service principal

05/03/2019 13:02:39 05/03/2019 23:02:39 krbtgt/DOMAIN.NAME@DOMAIN.NAME

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 administrator_name domain.name

#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, vi har kaldt gruppen: "SRV_OS2MO_(indsæt servernavn)_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

#Part 8 : Opsæt automatisk opsætning af Homedir

sed -i -e '/pam_sss.so/a \#Inserted by Script\nsession required pam_mkhomedir.so skel=/etc/skel/ umask=0077\n#End Inserted by Script' /etc/pam.d/common-session 1. Og sikrer os at de grupper vi ønsker har adgang til at køre kommandoer som super user.

#Part 9 : 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 10 : 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

Ud over OS2MO Serveren har vi 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 til dette, kan være en Windows Server 2016 (eller nyere) med Remote Administration værktøjer til bl.a. AD og jvad der ellers skal sendes eller trækkes data fra..

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 (PowerShell Remoting)

Vi har oprettet en specifik service konto (AD konto), som OS2MO AD integrationen anvender til at eksekvere PowerShell på Management serveren med. Denne service konto er medlem af "Remote Management Users" gruppen på serveren så den kan forbinde via PowerShell til 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 eller MitID og til MFA på 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

Connection Settings
Name: Schema
Path: LDAP:/
Connection Point
O Select or type a Distinguished Name or Naming Context:
v
Select a well known Naming Context:
Schema 🗸
Default naming context Comp(gration Comp(sotDSE
O Se Schema
v
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced OK Cancel

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

Console1 - [Co	onsole Root\ADSI Edit\Sche	ma (=	In a related institution of the family of the field	MUC-test	- - x
🖀 File Action View Favorites Windo	w Help				_ 8 ×
🗢 🔿 🙍 📰 💥 🗊 🔒 📓 📰					
Console Root	Name	Class	Distinguished Name ^	Actions	
4 🧟 Active Directory Schema	Construction of the local diversion of the local diversion of the local diversion of the local diversion of the	and solution.	Checkle Canada Checkman, National president 2014 (2018) 2014 and	CN-Schema CN-Confi	ouratio 🔺
Classes	Constraints on Spile.	and sold in	Construction of the Associate Construment Statistical protocolity on the	Mar Artices	guiutio
Attributes	and the second se	and sold as	Construction of the second state of the	More Actions	
A Z ADSI Edit	A DESCRIPTION OF THE OWNER.	1000 BOR 8		CN=xAttrCPR	
A Schema	A CONTRACTOR OF	100.00	the second se	More Actions	•
CN=Schema,CN=Configuratio	Section Section 2.	100.00	The state of a second state of the second particular with the state of the second se	more sectoris	
	and the strength of the streng	and shakes	The tasks of the barrier of the barrier part and the UK SHORE SHORE AND		
	Children Station	and solution	Charlen to the Charles Charles and the Charles		
	Contractor Station 18	and solution.	Charlense Rander Hills Street in Longenture Contractory		
	Children Station in	and sold a	Our region is a description of the low of protocol state and the low		
	Contraction and	Real Property in	Complete the or second conjuster in the second		
	A CONTRACTOR OF THE OWNER.	And the state of			
	and the local sector of	Second Second	the same of the set of		
	the local sectors will be a sector of the	All shares of the	The same installed dates for a factor of the billing of the		
	Contraction of the local division of the loc	and the second	The lines have been the second second second second second second		
	The second second second	and solution	Christian Spain Schemer Schemer Street and Schemer Street Street Schemer S		
	Christian Chrysel	and solution	Christen Compacitie Latera Christepaster, Contral Million -		
	Constant Center	and a second	Christen Caste On Several Include particular in Williams		
	CARLES AND A DESCRIPTION	server servers.	Construction and the second state of the secon		
	A CONTRACTOR OF	1000 ALC: N	the state way have been also and the state of the state o		
	State of the Party	100.000	The second s		
	Statement of the statement	and the second	The Property of the Association of the Property of the Propert		
	Contraction of the local division of the	and the second	The difference of the later of the later of the later of the difference of the later of the late		
	Concernance of the second	and the second second	Charles Carl Charles and Charles and Charles and Charles and Charles and		
	CN=xAttrCPR	attributeSch	CN=xAttrCPR, CN=Schema, CN=Configuration,		
< III >	Move				
	Delete]]	
Opens the properties alalog box for the current	Rename				
	Properties				
	Help				
				Mindows Se	$r_{vor} 20$

I properties find og vælg "searchFlags" og tryk på Edit

ttributes:		_
Attribute	Value	^
replPropertyMetaData	AttID Ver Loc.USN Org.DSA	
replUpToDateVector	<not set=""></not>	
repsFrom	<not set=""></not>	
repsTo	<not set=""></not>	
revision	<not set=""></not>	
schemaFlagsEx	<not set=""></not>	
schemalDGUID	0a85769c-db27-42f1-b415-0142dfa08a2a	
searchFlags	0x0 = ()	
showInAdvancedVie	TRUE	
subRefs	<not set=""></not>	_
systemFlags	<not set=""></not>	=
systemOnly	<not set=""></not>	
hu	<not set=""></not>	
uSNChanged	150810069	V
< 111	>	•

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.

	Integer Attribute Ed	ditor	×
Attribute: Value:	searchFlags		
Clear		ОК	Cancel

Når den er sat vises følgende I searchFlags feltet

searchFlags 0x80 = (CONFIDENTIAL)

Tryk OK for at gemme opsætningen.

For at sætte adgang til attributten op skal 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 i den næste dialogboks

	Bin	d		x
licer:				
Password:				=
Domain:				- 1
Rind tune				
 Bind as curre 	ntly logged	on user		
O Bind with cre	dentials			
○ Simple bind				
O Advanced (D	IGEST)			
Encrypt traff	fic after bin	d		
		Cancel	OK	
0.dvanced				

Vælg View og Tree



Vælg DC=Domain,DC=Name og tryk OK



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

R			Idap://
Connection Brows	se View Options	Utilities	Help
──OU=_S ──OU=Ac	Search Virtual List View	Ctrl+S	
OU=Ac OU=Ar OU=Br CN=BL CN=Cc OU=Dc	Delete Modify Modify DN Add child	Ctrl+D Ctrl+M Ctrl+R Ctrl+A	
- OU=Fa - CN=Fo	Advanced		Replication Metadata
OU=Fo CN=Int CN=Lo	Copy DN Copy Select all	Ctrl+C	Security Descriptor
CN=M OU=M	Clear output	Ctrl+N	and an effect of the second se

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: NT AUTHOR	RITY\SELF		
ACE type: Allow	O Deny O Audit	Alarm	
Access mask Read property List List object Read permissions	Write property Write DACL Write owner Write SACL	Create child Delete child Delete Delete Delete tree	Control access
ACE flags ☑ Inherit ☑ No propagate	Inherited	Success	
Object type:	xAttrCPR - attribute	•	~
Inherited object type:	user	01	~

Denne giver brugeren selv lov til at se xAttrCPR attributten på egen AD bruger.

Trustee: DOMAIN\ADUC_Brugere_xAttrCPR_Read

ACE - Access Control I	Entry		×
Trustee:	ADUC_Brugere_xAtt	rCPR_Read	
ACE type: Allow Access mask	O Deny O Audit		
Read property List List List object Read permissions	Write property Write DACL Write owner Write SACL	Create child Delete child Delete Delete Delete	Control access
ACE flags Inherit No propagate	Inherited	Success	
Object type: Inherited object type:	xAttrCPR - attribute	2	~
		ОК	Cancel

Trustee: DOMAIN\ADUC_Brugere_xAttrCPR_Modify

ACE - Access Control Entry X					
Trustee: ADUC_Brugere_xAttrCPR_Modify					
ACE type: Allow	O Deny O Audit	Alarm			
Access mask Read property List List object Read permissions	Write property Write DACL Write owner Write SACL	Create child Delete child Delete Delete	Control access		
ACE flags Inherit No propagate	Inherited	Success			
Object type: Inherited object type:	xAttrCPR - attribute	2	~ ~		
		OK	Cancel		

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

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 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 bl.a. medlem af gruppen der tildeler adgang til at læse og skrive i CPR-nummer attributten på brugere.