

Active Directory Migration Tool, versie 3.

Walter van der Horst.

Veel migraties en consolidaties van Windows NT omgevingen zijn uitgevoerd met de vorige versie de Active Directory Migration Tool (ADMT), versie 2. Enkele maanden geleden is er een nieuwe versie van deze tool beschikbaar gekomen, ADMT v3. Dit artikel bespreekt een aantal van de meest opvallende wijzigingen in ADMT v3 in vergelijking met ADMT v2. Er worden ook enkele tips gegeven aan de hand van ervaringen die zijn opgedaan tijdens het gebruik van ADMT v3.

Vorbereiding en installatie

In de voorbereiding en installatie voor ADMT is niets gewijzigd. Er moet nog steeds een two-way trust bestaan tussen de source (NT) en target (Active Directory) domeinen.

Tip: Het kan voorkomen dat er zich problemen voordoen met het opzetten van de trust tussen een Windows NT 4.0 domein en een Active Directory domein met Windows 2003 SP1 domein controllers. In Microsoft artikel KB 889030. Maak de aanpassingen besproken in het artikel in een separaat Group Policy Object (GPO), zodat de instellingen achteraf weer eenvoudig verwijderd kunnen worden.

Let wel, de aanpassingen gaan ten koste van de beveiliging van het Windows 2003 domein, dus zodra de trust niet meer nodig is deze settings verwijderen.

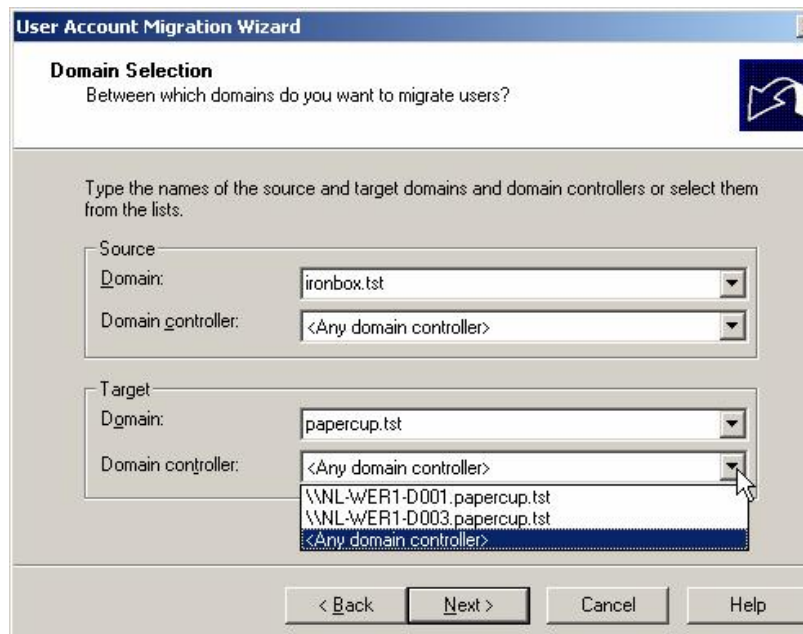
De "domain admins" global group uit het Windows NT 4.0 domein dient lid gemaakt te worden van de "administrators" local groep in het Windows Active Directory domein en vice versa.

Wat niet in de ADMT v3 help file terug is te vinden (er is ook geen documentatie beschikbaar, informatie kan gevonden worden in de ADMT v2 documentatie of de ADMT v3 helpfile) is dat ADMT geïnstalleerd en uitgevoerd moet worden vanaf een domein controller die global catalog (GC) is in het target domein. Indien dit niet het geval is doen er zich "access denied" foutmeldingen voor tijdens de migratie van computers.

De locatie van de ADMT v3 installatie files is niet langer "program files" maar C:\WINDOWS\ADMT.

Domeinselectie

Het eerste wat opvalt na de installatie van ADMT v3 en het opstarten van de een migratie is dat de mogelijkheid van het uitvoeren van een test migratie niet meer bestaat. Na het welkomtscherm verschijnt direct het domeinselectie scherm waarin de source en target domeinen geselecteerd kunnen worden. In dit scherm is direct een eerste verbetering zichtbaar. Het is nu mogelijk een domein controller te selecteren uit de source en target domeinen waar de migratie tussen plaats gaat vinden.



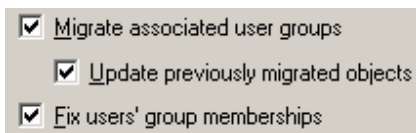
In de vorige versie van ADMT kon er geen invloed op de keuze van de domein controller worden uitgeoefend. Normaal gesproken was de PDC van het source domein de domein controller waar de object (gebruikers, computers) informatie vandaan werd gehaald. De domein controller waar ADMT op werd uitgevoerd was dan de machine waar deze informatie naartoe werd gemigreerd.

Dat is geen probleem zolang de verbindingen tussen de beide domein controller goed zijn. Echter, indien er grote afstanden over betrekkelijk langzame WAN verbindingen afgelegd moesten worden, kon de migratie van objecten nogal wat tijd in beslag nemen. Met ADMT v3 is het dus mogelijk twee domein controllers te selecteren die een goede onderlinge verbinding hebben.

Include file

Een andere wijziging is dat objecten nu ook uit een zogenaamde include file geselecteerd kunnen worden vanuit de userinterface. Een include file is een text file met hierin een lijst van de objecten (gebruikers, computers en groepen) die gemigreerd moeten worden. Dit is vooral handig als er grote aantallen objecten gemigreerd moeten worden.

Tip: Kies er tijdens het migreren van de gebruikers voor om groepen tegelijk met de gebruikers te migreren. Op deze manier migreer je alleen de groepen die ook gevuld zijn met gebruikers en de lege, en dus ongebruikte groepen, blijven achter. Op deze manier schoon je de infrastructuur op een eenvoudige manier op.



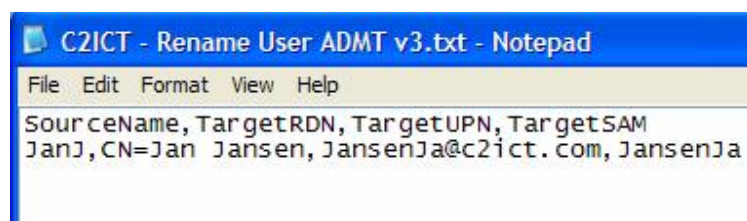
Het gebruik van een include file geeft ook de mogelijkheid om de objecten te renamen tijdens de migratie. Een rename was weliswaar in ADMT v2 ook al mogelijk. Maar er kon slechts een prefix of een suffix aan de naam worden toegevoegd, die ook nog eens gelijk was voor alle objecten die gemigreerd werden.

Met het gebruik van een include file is het dus mogelijk alle te migreren objecten van een nieuwe naam te voorzien.

Gebruikers hernoemen

Het gebruik van de rename optie wordt in de include file gedefiniëerd. Door extra headers op te nemen in de include file kan gebruikt gemaakt worden van de rename optie. Het separatie karakter tussen de header opties is een komma “,”.

In het onderstaande voorbeeld wordt een user account naam gewijzigd van “JanJ” “JansenJa”.



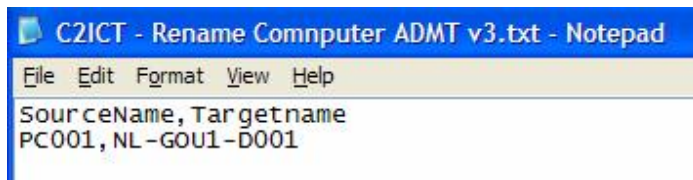
In de volgorde van de headers (SourceName, TargetRDN, etc.) is van belang dat de header "SourceName" vooraan moet staan. De volgorde van de overige drie headers doet er niet toe. Ter volledigheid volgt hieronder de relatie tussen de header optie het attribuut van het userobject in Active Directory:

- SourceName: De accountnaam in het Windows NT 4.0 domein.
- TargetRDN: Account naam van de gebruiker in Active Directory (dit is niet de displayname).
- TargetUPN: De "user logon name" in Active Directory (ook wel de UPN naam).
- TargetSAM: De "user logon name (pre-windows2000)" in Active Directory.

Computers hernoemen

Het hernoemen van een computer object gaat op dezelfde wijze als het hernoemen van een gebruiker. Het verschil zit hem in de header opties. Die zijn bij een computer object beduidend eenvoudiger. Er zijn dan maar twee headers nodig te weten, "SourceName" en "TargetName". Hierin zijn:

- SourceName: De computer naam in het Windows NT 4.0 domein.
- TargetName: De nieuwe computer naam in Active Directory.



Bij zowel ADMT v2 als ADMT v3 wordt er een agent gebruikt om een computer te migreren naar Active Directory. De agent wordt op de computer geïnstalleerd tijdens de migratie door ADMT. Tijdens dit proces is het dus van belang dat de bewuste computer te benaderen is. Met de agent in ADMT v3 is het mogelijk een zogenaamde pre-check uit te voeren. Er wordt dan gecontroleerd of the bewuste computer te benaderen is.

Tip: De firewall in Windows XP SP1 en Windows 2003 moet worden uitgeschakeld om het voor de ADMT agent mogelijk te maken de computer te benaderen. Ook VPN client software met ingebouwde firewalling (bijv.: Checkpoint VPN-1 SecureClient) moeten uitgeschakeld worden ten behoeve van de ADMT agent.

Conclusie

In dit artikel werden de meest in het oog springende wijzigingen aan ADMT v3 ten opzichte van ADMT v2 besproken. Vooral de mogelijkheid tot het selecteren van een voorkeurs domein controller en het kunnen aanpassen van (grote aantallen) gebruikers en werkplekken gedurende de migratie zijn verbeteringen die iets toevoegen aan het product. Migrators die veel ervaring hebben met ADMT v3 zullen gauw gewend zijn aan de wijzigingen die hebben plaatsgevonden.