krbtgt Password Reset

Wenn eine Domäne aufgesetzt wird, ist das Passwort des Key Distribution Center Service Account „KRBTGT", so alt wie der erste Domain Controller der in Betrieb genommen wurde.

Wenn die Domäne beispielsweise 5 Jahre läuft, dann ist auch das Passwort 5 Jahre alt.

Ist das sicher?

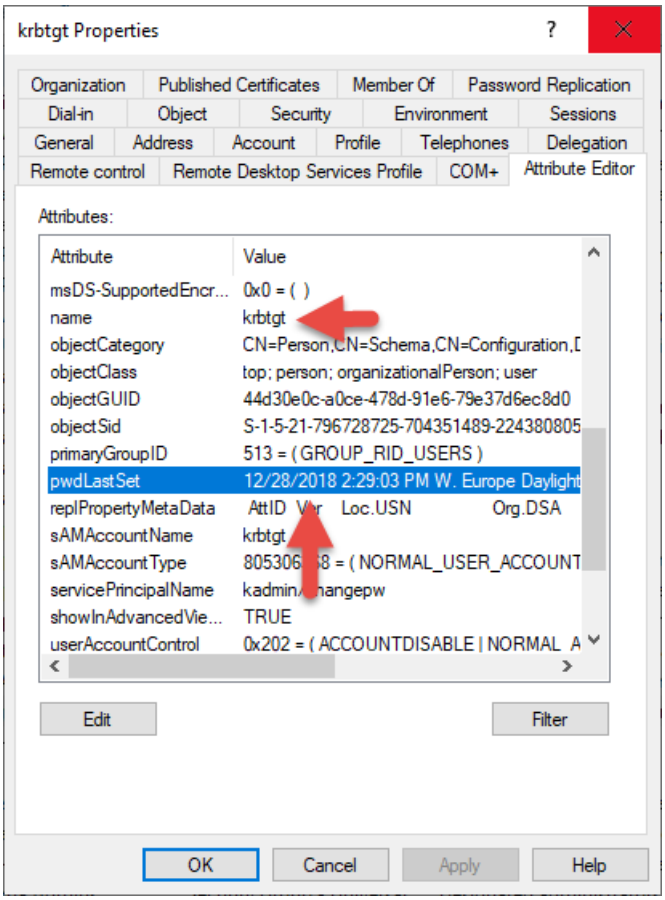
Was wenn der KRBTGT Master-Key bereits kompromittiert wurde?

Aus diesem Grund gehört das Passwort genauso oft gewechselt, wie das Passwort eines Admins, also spätestens alle 90 Tage. Besser noch alle 30 Tage.

Keine Sorge, das Passwort lässt sich ohne weiteres und ohne Probleme ändern.

Die Gültigkeit des Passworts liegt bei 10 Stunden und der Domaincontroller ist in der Lage sich 2 Kennwörter für diesen Account zu merken. Somit bleiben die bereits ausgestellten TGTs der letzten 10 Stunden gültig. Niemand muss sich nach dem Ändern des KRBTGT Kennworts neu authentifizieren.

Das Kennwort ist nun seit dem 28.12.2018 nicht mehr geändert worden. Das hole ich jetzt nach. Das Ganze lässt sich manuell an einem DC erledigen, denn das Passwort wird kurz darauf innerhalb der Domäne zu allen DCs repliziert.

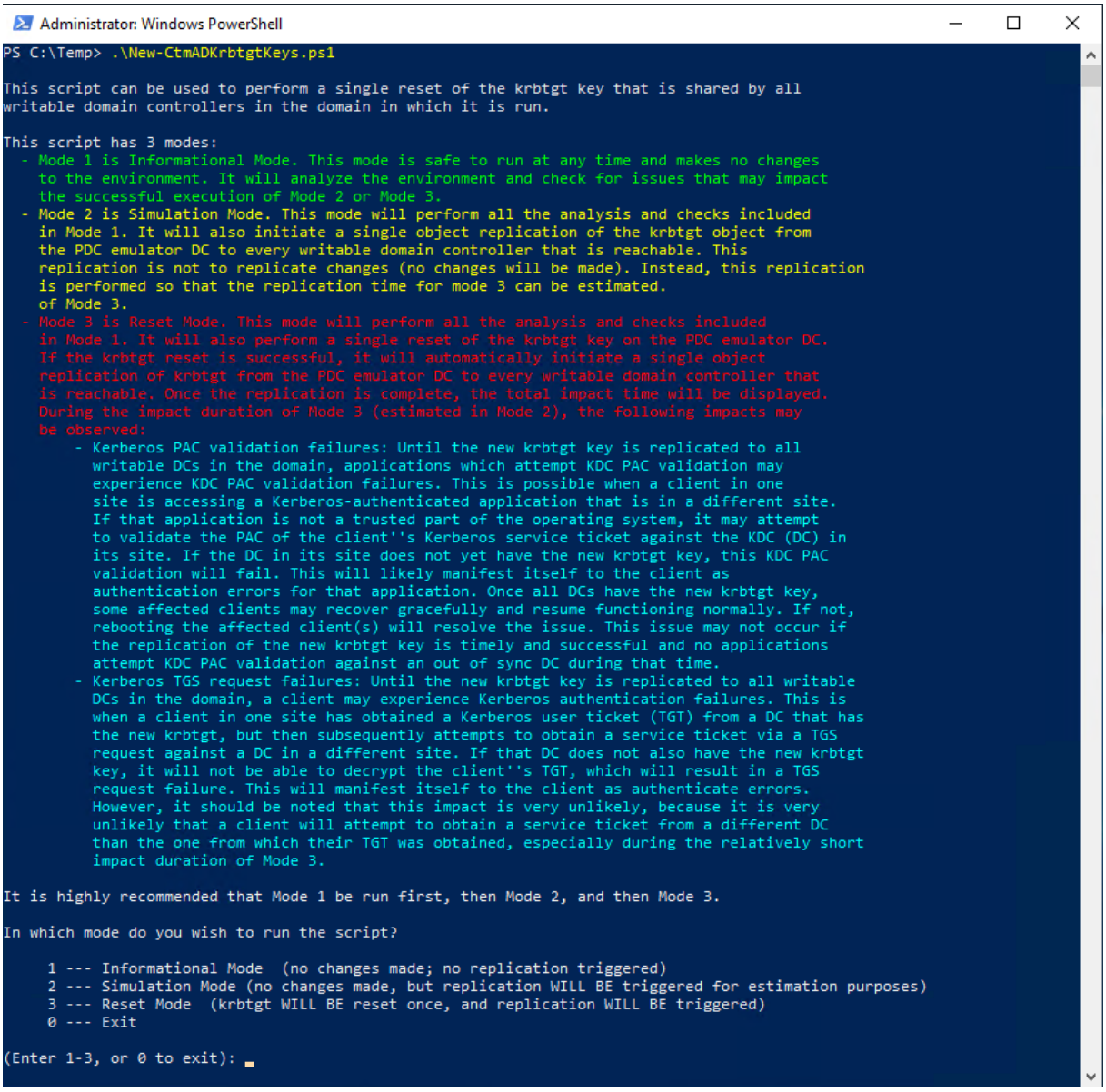


krbtgt Password Reset

Man kann aber auch ein Skript aus dem Technet einsetzen. Dieses Skript läuft in 3 Schritten ab. Der erste Schritt dient zur Information, der 2. Schritt der Simulation und der 3. Schritt ändert das Passwort und startet die Replikation.

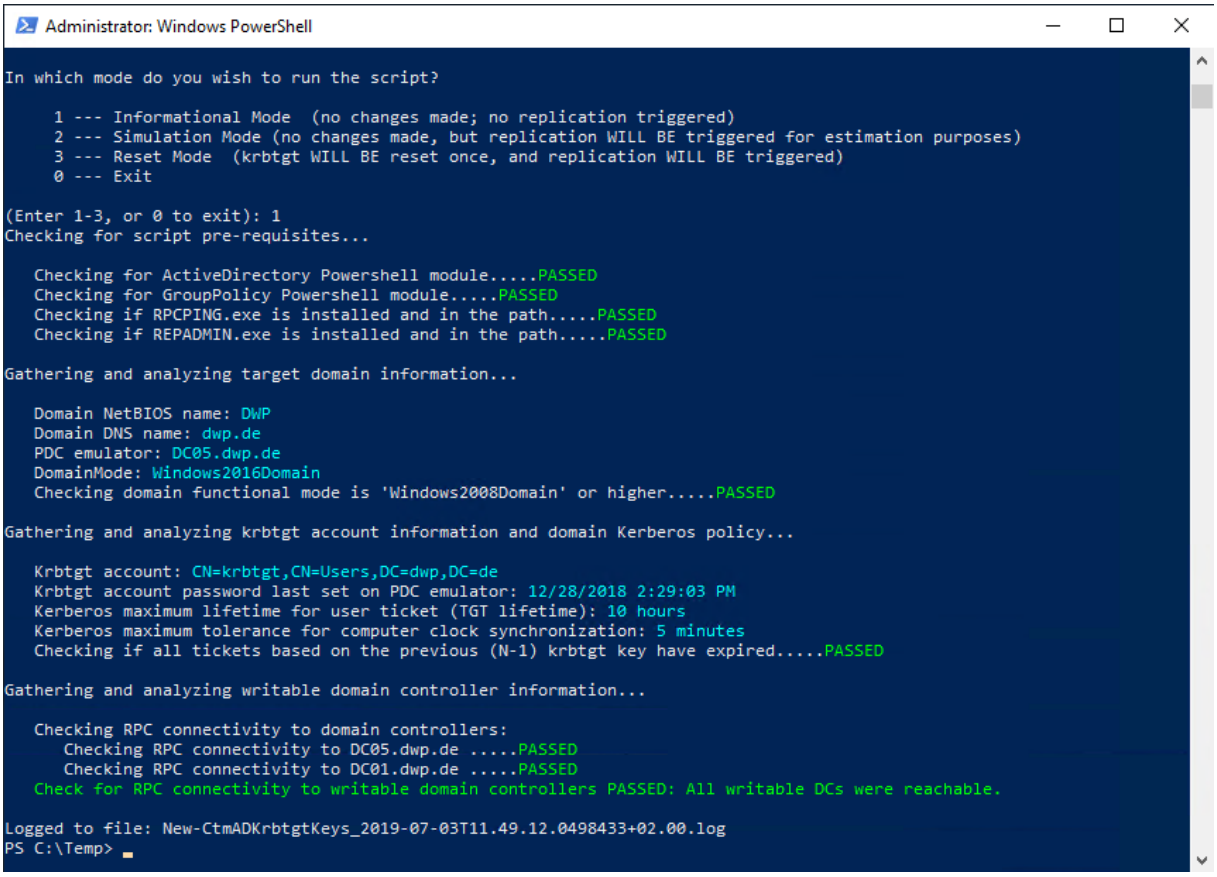
https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Ich starte das Skript und es werden mir 3 Schritte angeboten.

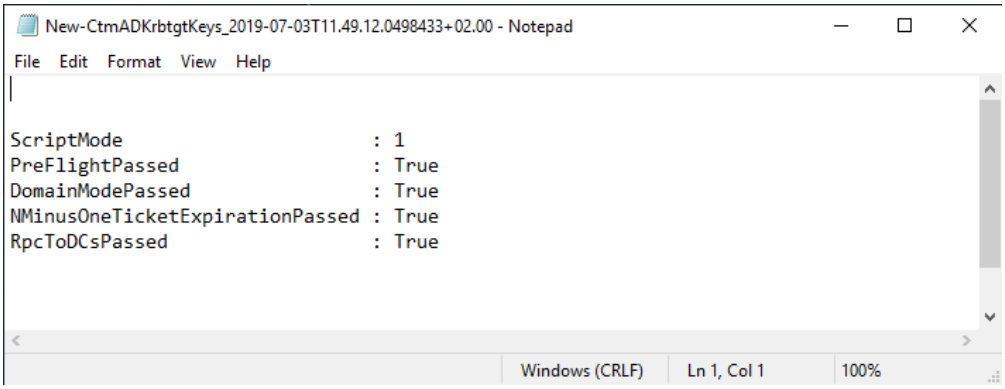


krbtgt Password Reset

Zuerst lesen wir die Informationen rund um die Domäne, Erreichbarkeit, Domänenmodus, Funktionsebene, Ticket-Lifetime usw. aus.



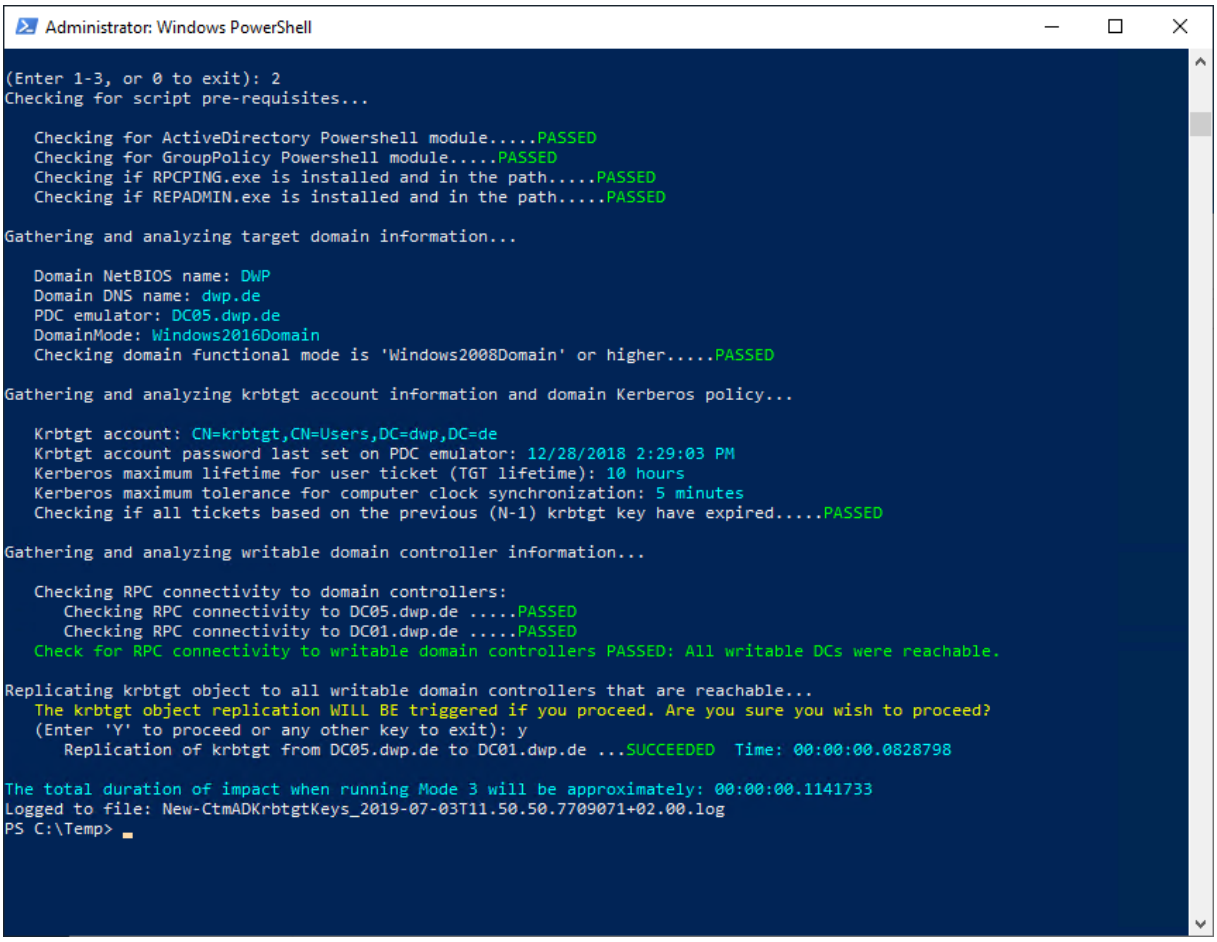
Zu jedem Schritt wird ein Log geschrieben.



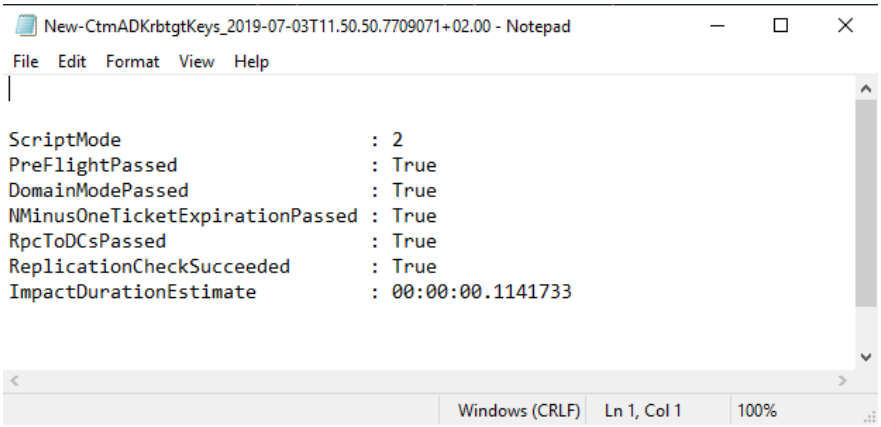
krbtgt Password Reset

Starte das Skript noch einmal und fahre mit dem 2. Schritt fort.

Die Replikation, RPC Konnektivität wurde überprüft.



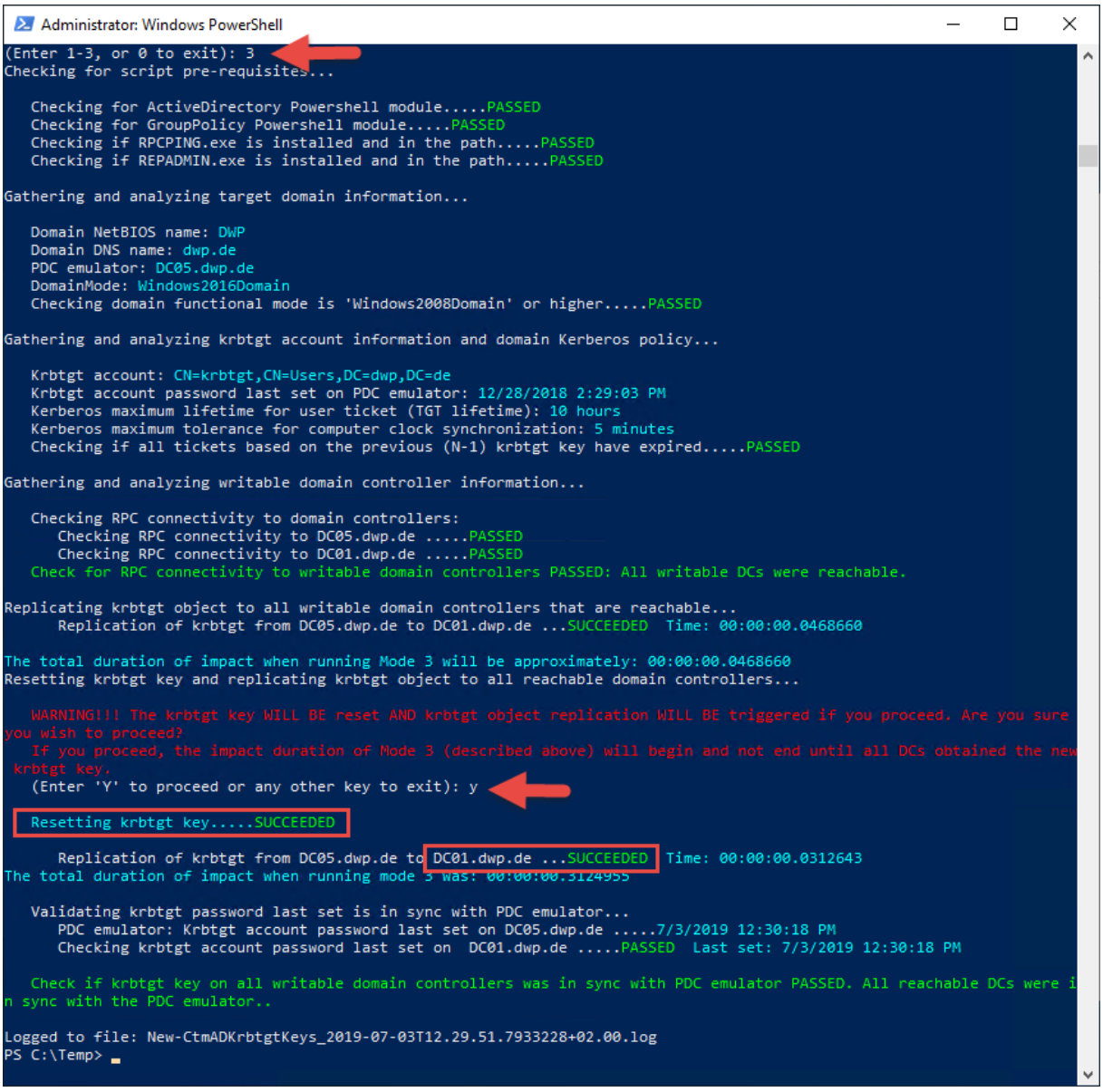
Das dazugehörige Log.



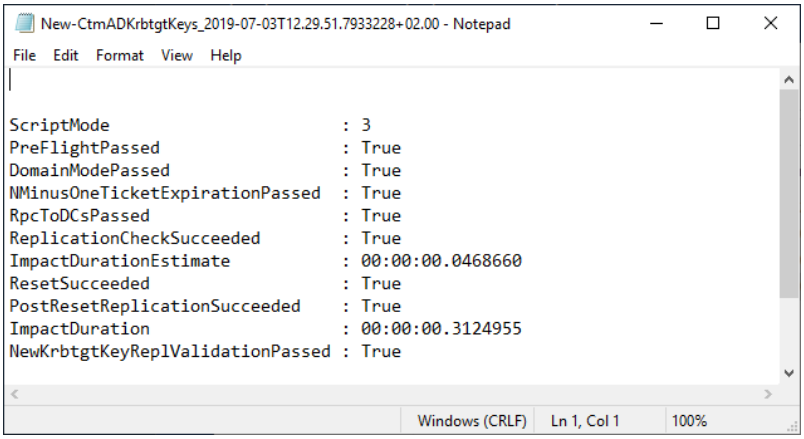
krbtgt Password Reset

Die Passwortänderung führen wir mit Schritt 3 durch.

Das Passwort wurde geändert und repliziert.



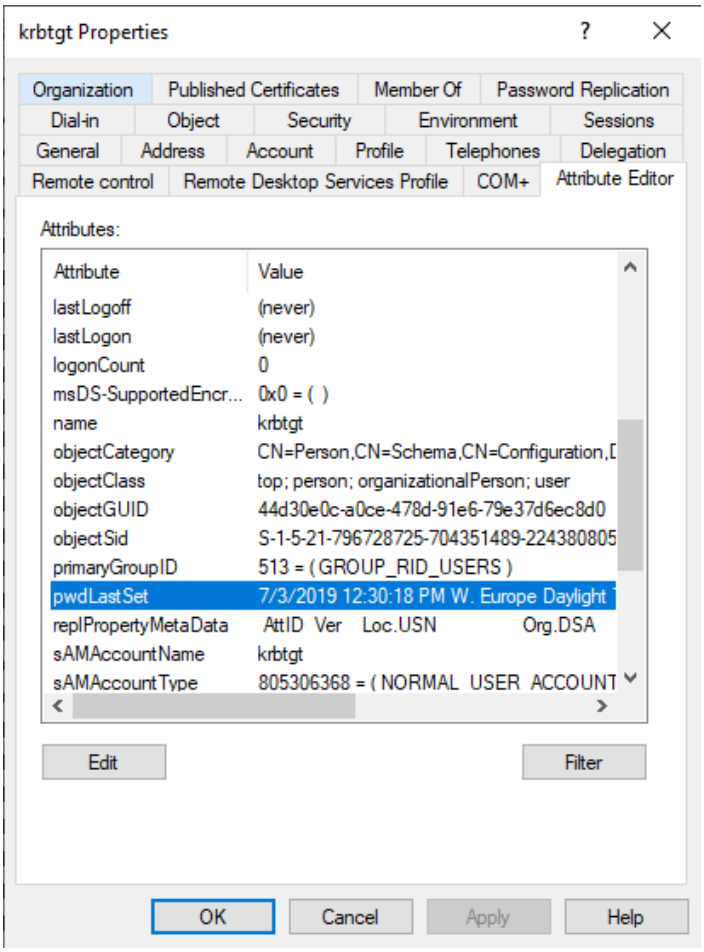
Auch hier ein Log:



krbtgt Password Reset

Überprüfe das Ganze auf dem 2. DC.

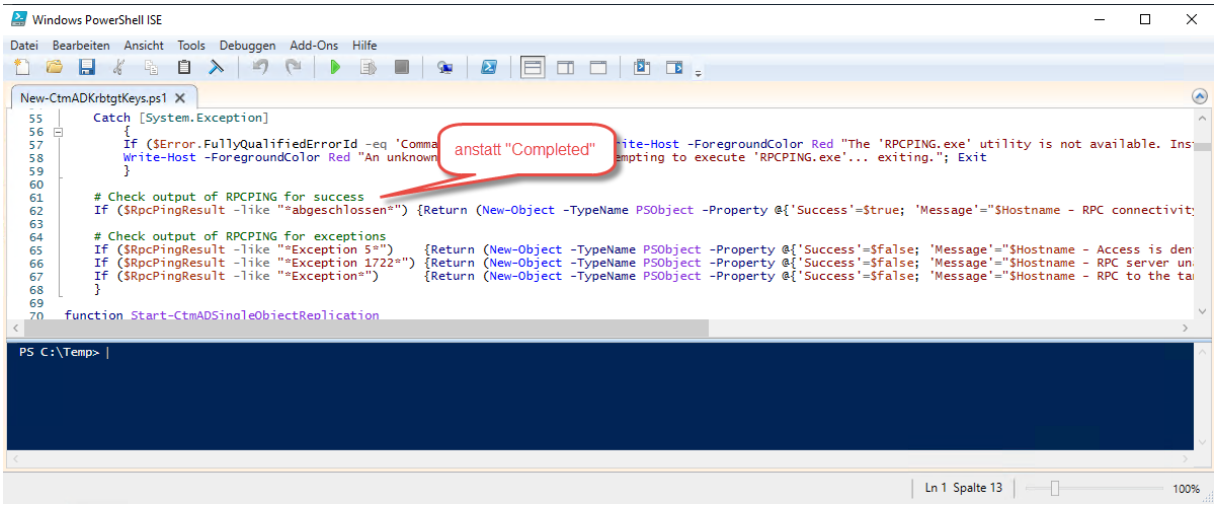
Die Änderung wurde sauber repliziert.



Die bereits ausgestellten TGTs (Session-Keys) werden mit dem alten Kennwort validiert und die neu auszustellenden Tickets mit dem neuen Kennwort des KRBTGT verschlüsselt.

Information:

Für ein deutsches OS muss in Zeile 62 eine kleine Anpassung stattfinden.



Erstellt von Jörn Walter **03.07.2019**

krbtgt Password Reset

Oder ganz klassisch über dieses Skript:

```
Import-Module ActiveDirectory
Set-ADAccountPassword -Identity (Get-ADUser krbtgt).DistinguishedName
-Reset -NewPassword (ConvertTo-SecureString "Ranm3xComP@ssw0rd!"
-AsPlainText -Force)
```