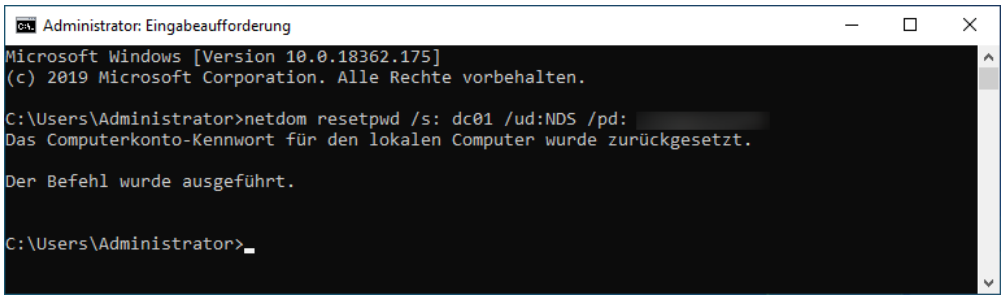
UserAccountControl 0x1020 PASSWD_NOTREQ

Eins meiner Clientsysteme (WIN10Client) wurde ausversehen aus dem AD gelöscht. Schnelle Hand wurde das Objekt wieder angelegt und das Passwort vom Client aus zurückgesetzt.

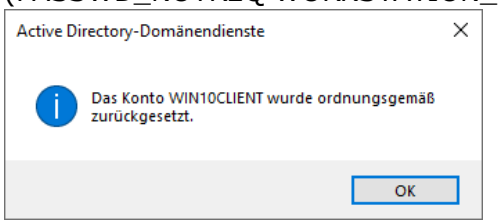
netdom resetpwd /s: dc01 /ud:NDS /pd: Passwort



Danach kontrollierte ich das Computer-Objekt anhand seiner Attribute. Da fiel mir auf, das unter dem Attribut „userAccountControl" der Wert 0x1020 stand. Dieser Wert ist = (PASSWD_NOTREQ WORKSTATION_TRUST_ACCOUNT).

Das bedeutet im Umkehrschluss, dass diesem Account vertraut wird, obwohl kein Passwort hinterlegt ist. Somit sollte doch auch kein Secure Channel zum AD Controller aufgebaut werden können?!

Auch ein Reset des Accounts (Konto zurücksetzen) hat nichts an dem Status (PASSWD_NOTREQ WORKSTATION_TRUST_ACCOUNT) geändert!

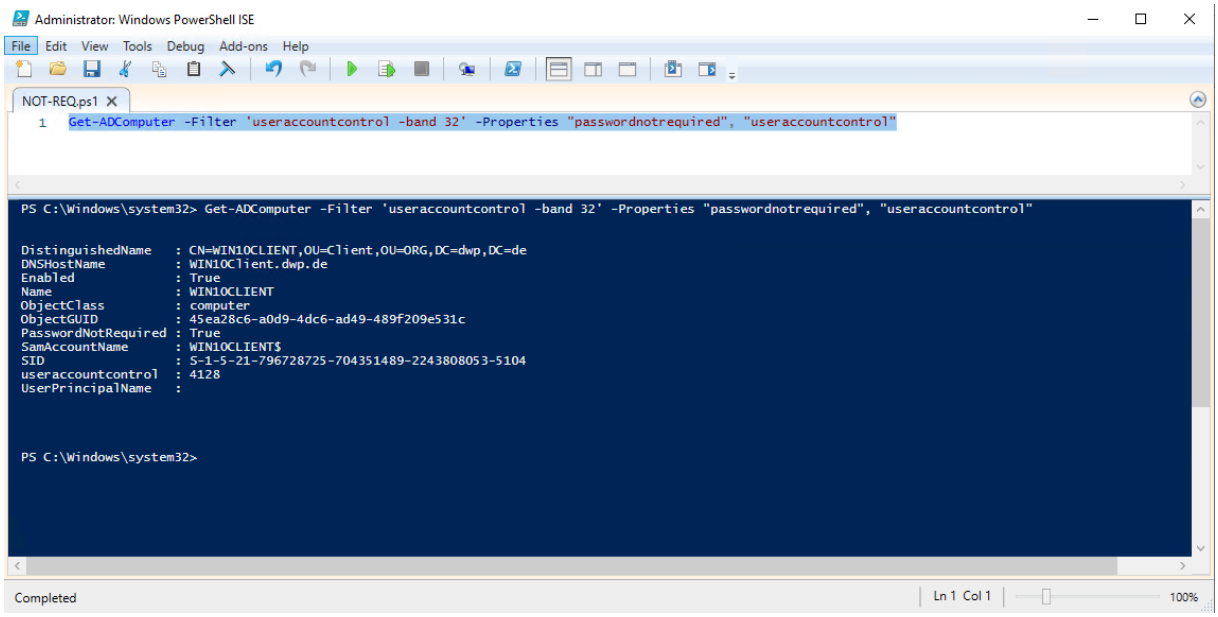


Außer, dass das Computer-Objekt die Vertrauensstellung verloren hat.

UserAccountControl 0x1020 PASSWD_NOTREQ

Also habe ich mit Hilfe der Powershell mal überprüft, ob noch mehrere Computer-Objekte betroffen sind:

Get-ADComputer -Filter 'useraccountcontrol -band 32' -Properties "passwordnotrequired", "useraccountcontrol"



Vertrauenswürdige Werte:

Der Wert der dort eigentlich stehen sollte lautet für Workstation: 0x1000 (4096)

Der Wert der dort eigentlich stehen sollte lautet für Member Server: 0x1000 (4096)

Der Wert der dort eigentlich stehen sollte lautet für Domaincontroller: 0x82000 (532480)

Nicht Vertrauenswürdige Werte:

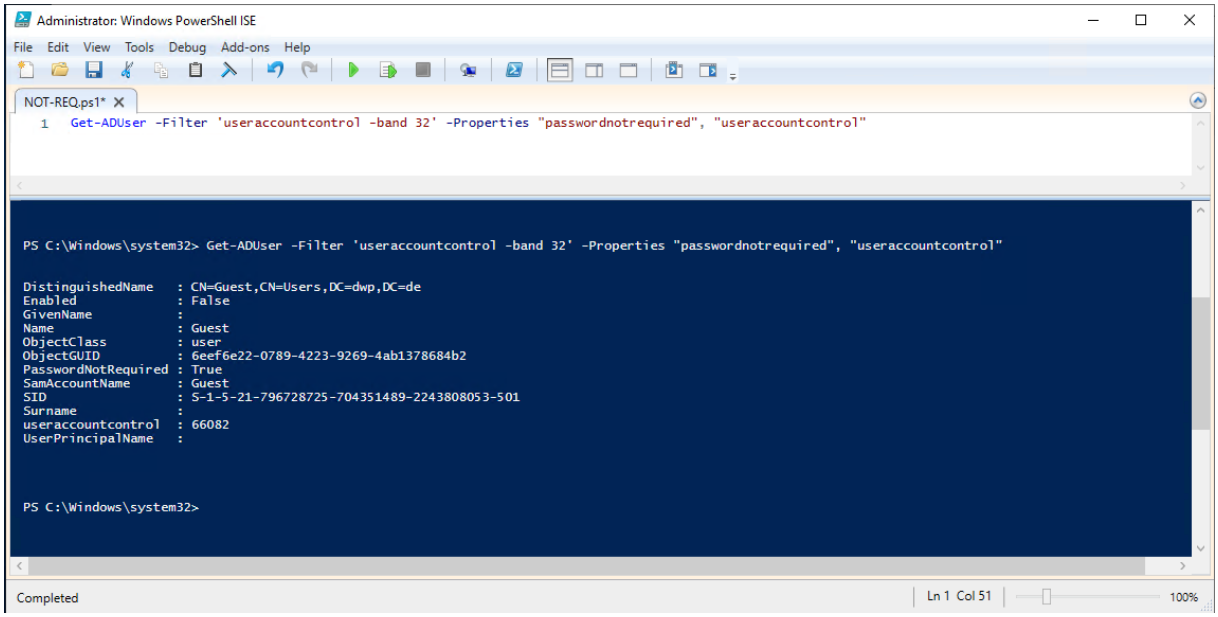
Dieser Wert sollte bei Domaincontrollern nicht stehen: 0x82020

Dieser Wert sollten bei Workstations und Member Servern nicht stehen: 0x1020

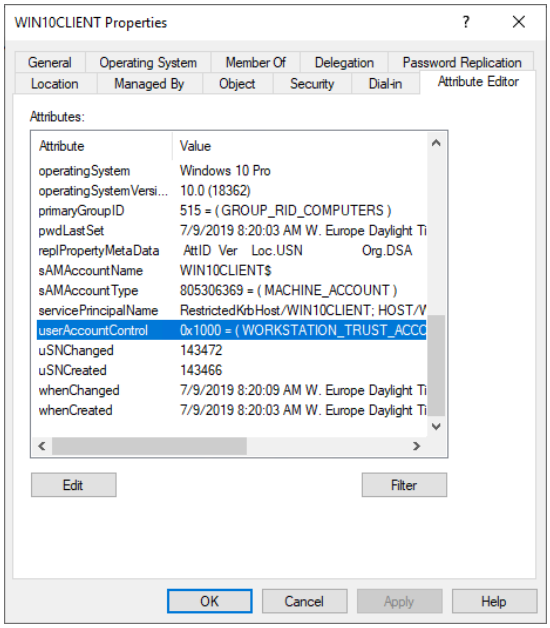
UserAccountControl 0x1020 PASSWD_NOTREQ

Auch Benutzer könnten in diesem Zuge mal mit überprüft werden.

Get-ADUser -Filter 'useraccountcontrol -band 32' -Properties "passwordnotrequired", "useraccountcontrol"

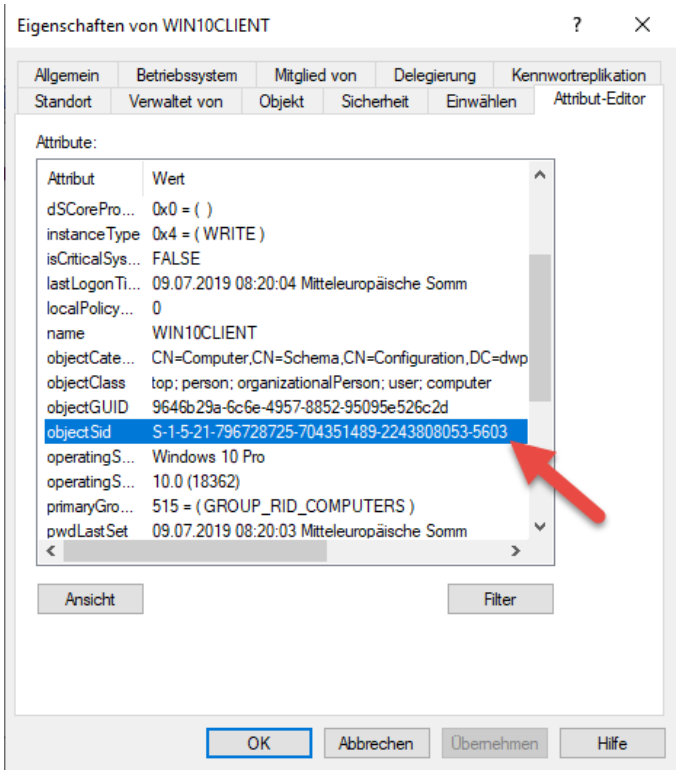


Wenn ich die Workstation nach dem es die Vertrauensstellung verloren hat, über die eigene Computerverwaltung korrekt aus der Domäne enthebe und diese anschließend wieder aufnehme, wird der Wert im Attribut „userAccountControl" mit 0x1000 ausgegeben, also als Vertrauenswürdig eingestuft.



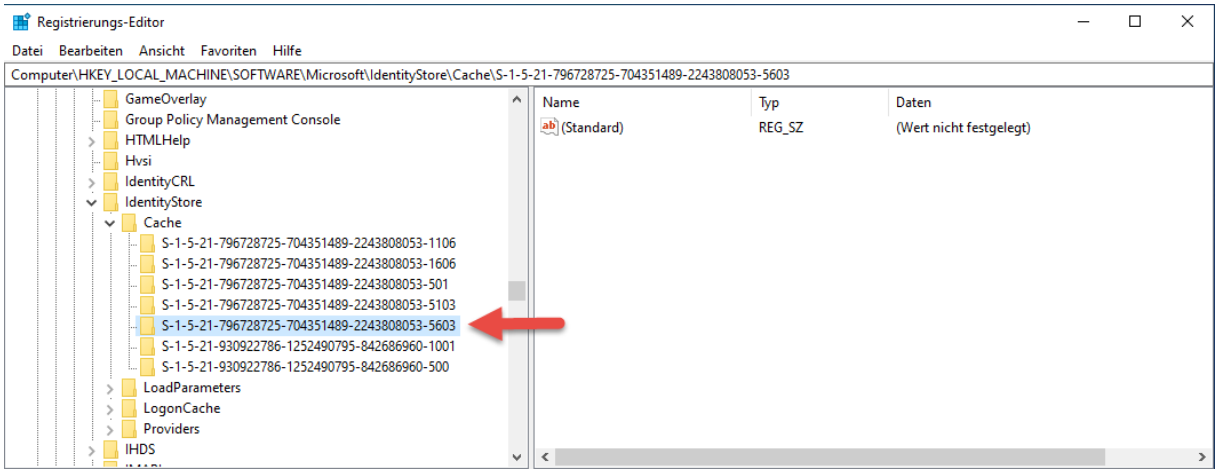
Mit jedem Beitritt in eine Domäne nimmt ein Objekt in diesem Fall ein Computer eine neue Identität an. Ausgewiesen durch das Attribut „objectSid" (SID) Security Identifier.

UserAccountControl 0x1020 PASSWD_NOTREQ



Die „objectSid" finde ich auf dem Computer-Objekt in der Registry unter dem Schlüssel „IdentityStore" wieder.

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IdentityStore\Cache



Die „objectSid" zusammen mit dem Computerkennwort werden zum Authentifizieren eingesetzt, genau wie bei einem Benutzer (UserID + Kennwort).

Fazit:

Was ich bis jetzt herausgefunden habe ist, dass das erneute Anlegen eines Computer-Objekts im AD, mit anschließendem Reset des Kennworts

netdom resetpwd /s: dc01 /ud:NDS /pd: Passwort

keine gute Wahl ist, um eine erneute Vertrauensstellung zu bewirken.

UserAccountControl 0x1020 PASSWD_NOTREQ

Liste mit Werten für das Attribut „userAccountControl"

Tagesgeschäft:

512	Enable Account
514	Disable account
544	Account Enabled - Require user to change password at first logon
4096	Workstation/server
66048	Enabled, password never expires
66050	Disabled, password never expires
262656	Smart Card Logon Required
532480	Domain controller

Alle anderen Werte:

1	script
2	accountdisable
8	homedir_required
16	Lockout
32	passwd_notreqd
64	passwd_cant_change
128	encrypted_text_pwd_allowed
256	temp_duplicate_account
512	normal_account
514	Disabled Account
544	Enabled, Password Not Required
546	Disabled, Password Not Required
2048	interdomain_trust_account
4096	workstation_trust_account
8192	server_trust_account
65536	dont_expire_password
66048	Enabled, Password Doesn't Expire
66050	Disabled, Password Doesn't Expire
66080	Enabled, Password Doesn't Expire & Not Required
66082	Disabled, Password Doesn't Expire & Not Required
131072	mns_logon_account

UserAccountControl 0x1020 PASSWD_NOTREQ

262658	Disabled, Smartcard Required
262688	Enabled, Smartcard Required, Password Not Required
262690	Disabled, Smartcard Required, Password Not Required
328192	Enabled, Smartcard Required, Password Doesn't Expire
328194	Disabled, Smartcard Required, Password Doesn't Expire
328224	Enabled, Smartcard Required, Password Doesn't Expire & Not Required
328226	Disabled, Smartcard Required, Password Doesn't Expire & Not Required
524288	trusted_for_delegation
1048576	not_delegated
2097152	use_des_key_only
4194304	dont_req_preauth
8388608	password_expired
16777216	trusted_to_auth_for_delegation
67108864	PARTIAL_SECRETS_ACCOUNT