gMSA Account – Installation failed

Ein Managed Service Account (gMSA oder sMSA), hier müssen wir zwischen zwei Arten unterscheiden. Zum einen gibt es die Managed Service Accounts, diese können nur von einem Computerobjekt eingesetzt werden. Man spricht an dieser Stelle auch von Single Accounts. Zum anderen gibt es noch die Group Managed Services Accounts. Diese können auf mehreren Computerobjekten eingesetzt werden.

Weitere Details zur Einrichtung und Installation findet ihr hier:

https://www.der-windows-papst.de/2019/02/12/unterschied-managed-service-account-group-managed-service-account/

https://www.der-windows-papst.de/2016/02/27/server-20102-group-managed-service-account-erstellen/

Die Installation eines Group Managed Services Accounts schlägt fehl!

Wenn folgende Fehlermeldungen erscheinen,

```
PS C:\Windows\system32> Install-ADServiceAccount gMSA-Skripte
Install-ADServiceAccount : Cannot install service account. Error Message: 'An unspecified error has occurred'.
At line:1 char:1
+ Install-ADServiceAccount gMSA-Skripte
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : WriteError: (gMSA-Skripte:String) [Install-ADServiceAccount], ADException
    + FullyQualifiedErrorId : InstallADServiceAccount:PerformOperation:InstallServiceAcccountFailure,Microsoft.ActiveDirectory.Management.Commands.InstallADServiceAccount
```

```
PS C:\Windows\system32> Test-ADServiceAccount gMSA-8Man
False
WARNING: Test failed for Managed Service Account gMSA-8Man. If standalone Managed Service Account, the account is linked to another computer object in the Active Directory. If
group Managed Service Account, either this computer does not have permission to use the group MSA or this computer does not support all the Kerberos encryption types required
for the gMSA. See the MSA operational log for more information.
PS C:\Windows\system32>
```

Hervorsticht der Hinweis bezüglich der Kerberos Encryption

```
the account is linked to another computer object in the Active Directory. If
or this computer does not support all the Kerberos encryption types required
```

dann liegt es sehr wahrscheinlich daran, dass die Server Hardening Richtlinie auf dem Domain-Controller wie folgt konfiguriert wurde.

Erlaubt ist nur noch die Nutzung von Kerberos in der Güte AES128 und AES256.

Other

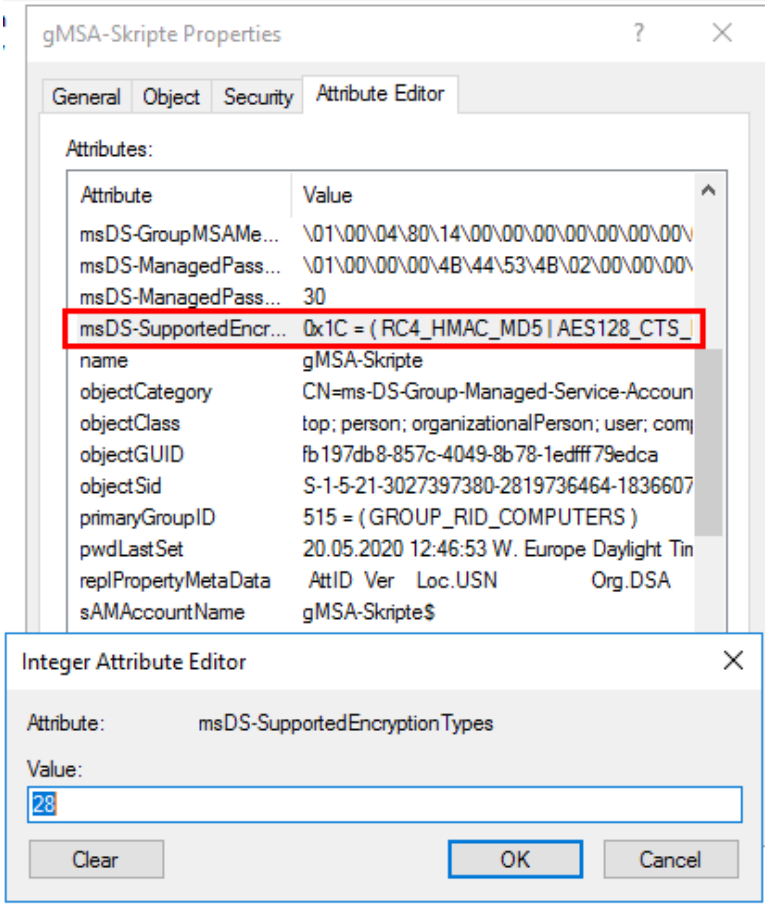
Policy	Setting
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Configure encryption types allowed for Kerberos	Enabled
DES_CBC_CRC	Disabled
DES_CBC_MD5	Disabled
RC4_HMAC_MD5	Disabled
AES128_HMAC_SHA1	Enabled
AES256_HMAC_SHA1	Enabled
Future encryption types	Enabled

Hinweis: Port 9389 muss natürlich immer freigeschaltet sein!

gMSA Account – Installation failed

Schauen wir uns einen eingerichteten Group Managed Service Account mal etwas näher an. Der Encryption Type trägt den Wert 28. Somit ist RC4_HMAC_MD5 gefolgt von AES128_CTS_HMAC_SHA1_96 und AES256_CTS_HMAC_SHA1_96 erlaubt.

Aber hier spielt die Reihenfolge eine große und sehr wichtige Rolle. Die obigen Fehlermeldungen (Warnings) sind Auslöser der voranstehenden RC4 Encryption. Die muss weg!



Gemäß der Hardening Policy des Domain-Controller stellen wir die Supported Encryption Types des gMSA-Accounts so ein, das nur noch AES128 und AES256 erlaubt ist.

Set-ADServiceAccount gMSA-8Man -KerberosEncryptionType AES128, AES256

```
PS C:\Windows\system32> Set-ADServiceAccount gMSA-8Man -KerberosEncryptionType AES128, AES256
```

Der Wert (Value) ändert sich nun von 28 auf 24

Anschließend lässt sich der Account installieren und testen.

Install-ADServiceAccount gMSA-8Man
Test-ADServiceAccount gMSA-8Man

```
PS C:\Windows\system32> Install-ADServiceAccount gmsa-8Man

PS C:\Windows\system32> Test-ADServiceAccount gmsa-8Man
True

PS C:\Windows\system32> |
```