Protected Users – geschützte Benutzer

Die Gruppe „Protected Users" oder „Geschützte Benutzer" hat ihre Zweckmäßigkeit seit Windows Server 2016 darin gefunden, enthaltene Benutzer zu schützen.

Und zwar werden die Konten, die dieser Gruppe angehören dahingehend eingeschränkt, das folgende Merkmale nicht mehr zur Verfügung stehen oder angepasst werden:

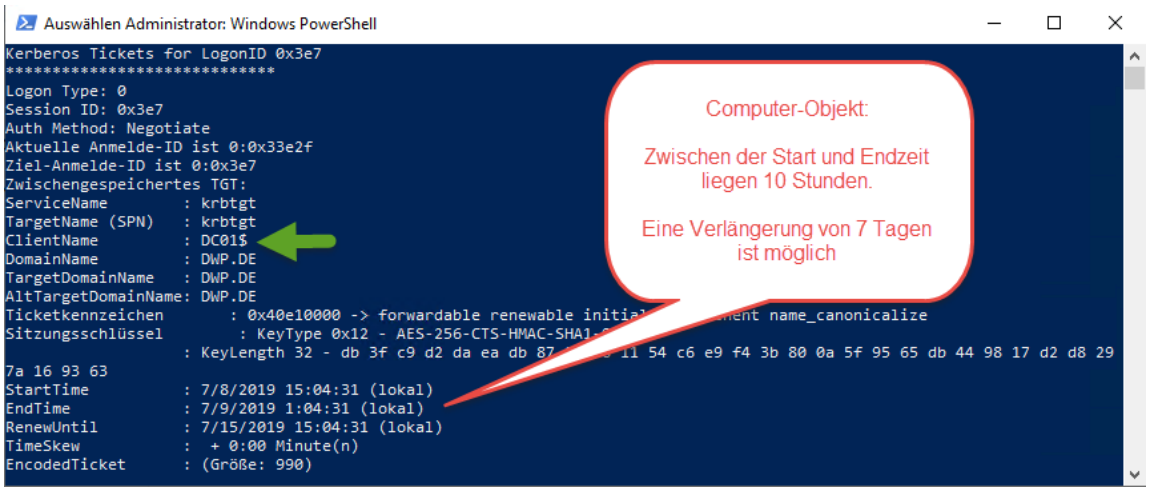
- Verwenden von zwischengespeicherten Anmeldungen, also keine Langzeitschlüssel mehr. Es folgt ab jetzt pro Anforderung ein Authentifizierungsvorgang
- Verwendung von NTLM, Digest-Auth und CredSSP
- Verwenden schwacher *Verschlüsselungsalgorithmen wie DES und RC4 für die Kerberos Pre-Authentication
- Verwendung von Kerberos Constrained und Unconstrained Delegation
- Gültigkeit des Kerberos Ticket Granting Ticket (TGT) nicht länger als 240 Minuten

Für die ersten 3 Punkte haben die meisten bereits Gruppenrichtlinien im Einsatz um die Merkmale einzuschränken. Gehört in jedes Hardening.

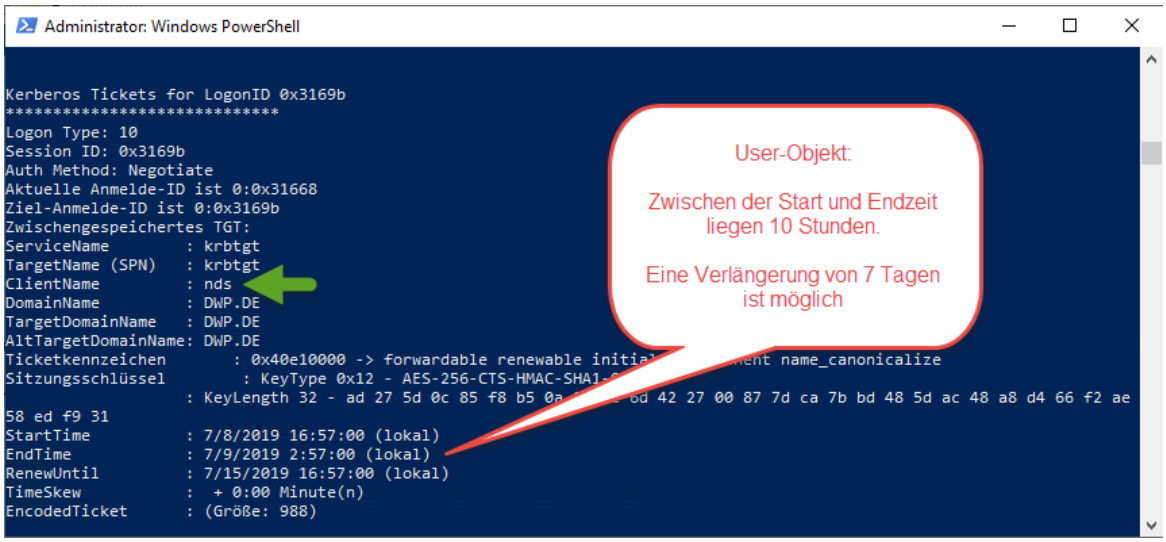
Gerne würde ich die Einschränkung zu Punkt 5 noch etwas besser darstellen wollen.

Standardmäßig, sofern nichts verändert wurde, hält ein TGT 10 Stunden und kann für 7 Tage verlängert werden. Sei es für Computer oder Benutzer.

Computer:



Benutzer:

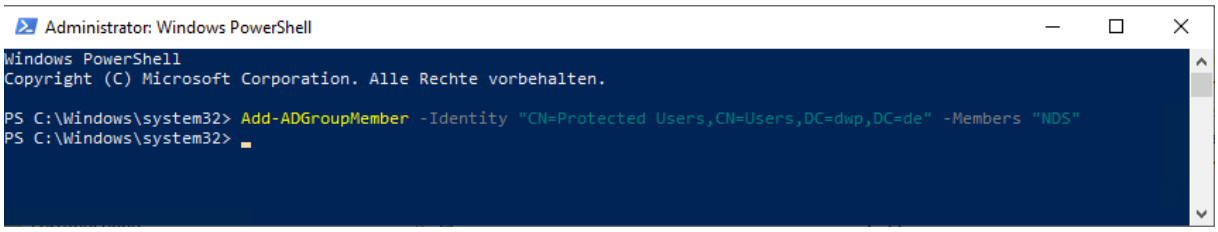


Protected Users – geschützte Benutzer

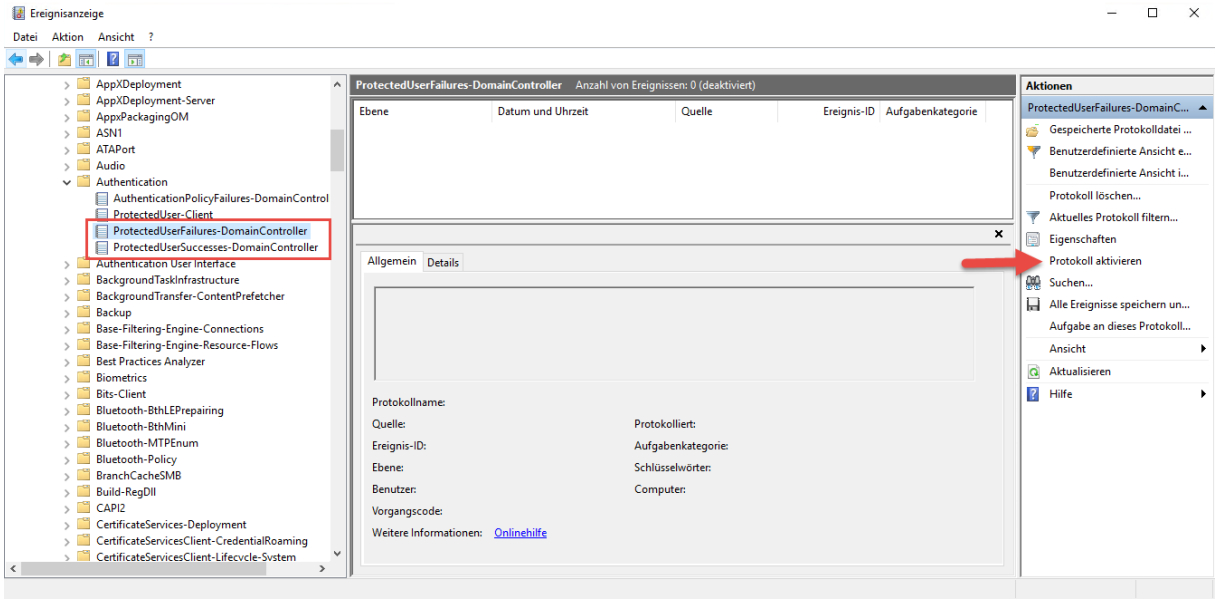
Sobald ein Benutzer Mitglied der Gruppe „Protected Users“ oder „Geschützte Benutzer“ wird, hält sein TGT wie oben bereits beschrieben nur noch 4 Stunden. Um die gleiche Zeit kann es auch maximal verlängert werden.

Mit Hilfe der Powershell wird der Benutzer „NDS“ Mitglied dieser besagten Gruppe.

```
Add-ADGroupMember -Identity "CN=ProtectedUsers,CN=Users,DC=dwp,DC=de" -Members "NDS"
```

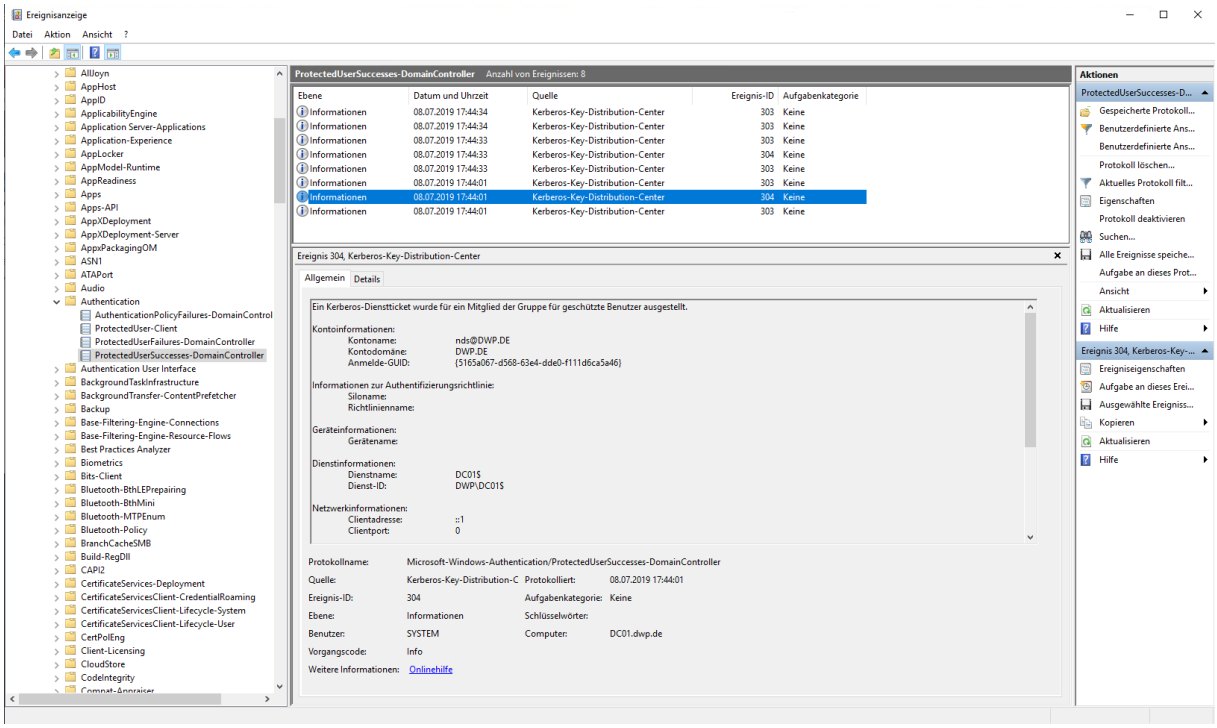


Zusätzlich sollte das Logging eingeschaltet werden.



Protected Users – geschützte Benutzer

Sobald de DC einem ProtectedUser ein Ticket ausgestellt hat, wird dieses entsprechend vermerkt:



Wichtige Info:

Nur privilegierte und sensitive Konten sollten Mitglied dieser Gruppe werden. Auf keinen Fall sollten MSA, gMSA oder Computer-Konten dieser „Geschützen Gruppe" angehören. Es kann zu Funktionsstörungen kommen!

*Sobald ein Benutzer Mitglied ist, muss sichergestellt sein, das die Authentifizierung mit Kerberos Advanced Encryption Standards kurz (AES) funktioniert.

Weitere Informationen zum Logging:

https://docs.microsoft.com/de-de/windows/security/threat-protection/auditing/event-4772

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn466518(v=ws.11)