



## 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:

```
Auswählen Administrator: Windows PowerShell
=====
Kerberos Tickets for LogonID 0x3e7
=====
Logon Type: 0
Session ID: 0x3e7
Auth Method: Negotiate
Aktuelle Anmelde-ID ist 0:0x33e2f
Ziel-Anmelde-ID ist 0:0x3e7
Zwischengespeichertes TGT:
ServiceName      : krbtgt
TargetName (SPN) : krbtgt
ClientName       : DC01$ ← Green Arrow
DomainName       : DWP.DE
TargetDomainName : DWP.DE
AltTargetDomainName: DWP.DE
Ticketkennzeichen   : 0x40e10000 -> forwardable renewable initial ticket name_canonicalize
Sitzungsschlüssel    : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                      : KeyLength 32 - db 3f c9 d2 da ea db 87 3c 11 54 c6 e9 f4 3b 80 0a 5f 95 65 db 44 98 17 d2 d8 29
7a 16 93 63
StartTime        : 7/8/2019 15:04:31 (lokal)
EndTime          : 7/9/2019 1:04:31 (lokal)
RenewUntil       : 7/15/2019 15:04:31 (lokal)
TimeSkew         : + 0:00 Minute(n)
EncodedTicket    : (Größe: 990)
```

Benutzer:

```
Administrator: Windows PowerShell
=====
Kerberos Tickets for LogonID 0x3169b
=====
Logon Type: 10
Session ID: 0x3169b
Auth Method: Negotiate
Aktuelle Anmelde-ID ist 0:0x31668
Ziel-Anmelde-ID ist 0:0x3169b
Zwischengespeichertes TGT:
ServiceName      : krbtgt
TargetName (SPN) : krbtgt
ClientName       : nds ← Green Arrow
DomainName       : DWP.DE
TargetDomainName : DWP.DE
AltTargetDomainName: DWP.DE
Ticketkennzeichen   : 0x40e10000 -> forwardable renewable initial ticket name_canonicalize
Sitzungsschlüssel    : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                      : KeyLength 32 - ad 27 5d 0c 85 f8 b5 0a 11 5d 42 27 00 87 7d ca 7b bd 48 5d ac 48 a8 d4 66 f2 ae
58 ed f9 31
StartTime        : 7/8/2019 16:57:00 (lokal)
EndTime          : 7/9/2019 2:57:00 (lokal)
RenewUntil       : 7/15/2019 16:57:00 (lokal)
TimeSkew         : + 0:00 Minute(n)
EncodedTicket    : (Größe: 988)
```



## 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.

```

Administrator: Windows PowerShell

Kerberos Tickets for LogonID 0x4c8c08
*****
Logon Type: 2
Session ID: 0x4c8c08
Auth Method: Negotiate
Aktuelle Anmelde-ID ist 0:0x4c8bdd
Ziel-Anmelde-ID ist 0:0x4c8c08
Zwischengespeichertes TGT:
ServiceName      : krbtgt
TargetName (SPN) : krbtgt
ClientName       : nds
DomainName       : DWP.DE
TargetDomainName : DWP.DE
AltTargetDomainName: DWP.DE
Ticketkennzeichen   : 0xe10000 -> renewable initial pre_authent
Sitzungsschlüssel    : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                        : KeyLength 32 - d5 92 fb 61 ee d4 2f 44 2e 26 df d2 78 56 d9 f7 ba 8f c3 bb d4 62 f9 09 45 20 fb
4b 4b fe e2
StartTime        : 7/8/2019 16:49:14 (lokal)
EndTime          : 7/8/2019 20:49:14 (lokal)
RenewUntil       : 7/8/2019 20:49:14 (lokal)
TimeSkew         : + 0:00 Minute(n)
EncodedTicket    : (Größe: 996)

```

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"**

```

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\system32> Add-ADGroupMember -Identity "CN=ProtectedUsers,CN=Users,DC=dwp,DC=de" -Members "NDS"
PS C:\Windows\system32>

```

Zusätzlich sollte das Logging eingeschaltet werden.

The screenshot shows the Windows Event Viewer interface. On the left, a tree view lists various log sources under 'ProtectedUserFailures-DomainController'. One specific entry, 'ProtectedUserFailures-DomainController', is highlighted with a red box. On the right, a detailed view of this log source is shown. A red arrow points to the 'Aktionen' (Actions) pane, specifically to the 'Protokoll aktivieren' (Enable Logging) option, which is also highlighted with a red box. The main pane displays a table with columns: Ebene, Datum und Uhrzeit, Quelle, Ereignis-ID, and Aufgabenkategorie.



## Protected Users – geschützte Benutzer

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

The screenshot shows the Windows Event Viewer interface. In the center pane, a list of events from the 'ProtectedUserSuccesses-DomainController' log is displayed. One event, with ID 304, is highlighted. The details pane shows the following information for this event:

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	08.07.2019 17:44:34	Kerberos-Key-Distribution-Center	303	Keine
Informationen	08.07.2019 17:44:34	Kerberos-Key-Distribution-Center	303	Keine
Informationen	08.07.2019 17:44:33	Kerberos-Key-Distribution-Center	303	Keine
Informationen	08.07.2019 17:44:33	Kerberos-Key-Distribution-Center	304	Keine
Informationen	08.07.2019 17:44:33	Kerberos-Key-Distribution-Center	303	Keine
Informationen	08.07.2019 17:44:01	Kerberos-Key-Distribution-Center	303	Keine
Informationen	08.07.2019 17:44:01	Kerberos-Key-Distribution-Center	304	Keine
Informationen	08.07.2019 17:44:01	Kerberos-Key-Distribution-Center	303	Keine

The details pane also contains a summary: "Ein Kerberos-Dienstticket wurde für ein Mitglied der Gruppe für geschützte Benutzer ausgestellt." Below this, various properties like Kontoname, Kontodomäne, and Dienstnamen are listed.

### Wichtige Info:

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

\*Sobald ein Benutzer Mitglied ist, muss sichergestellt sein, dass 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\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn466518(v=ws.11))