



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?

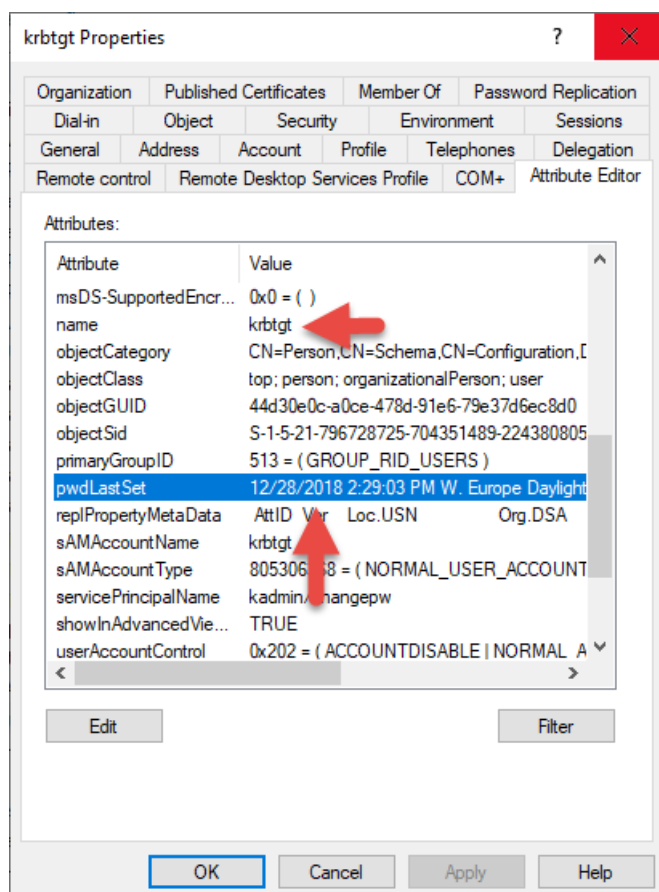
Was wenn der KRBTGT Master-Key bereits kompromittiert wurde?

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.

```
Administrator: Windows PowerShell
PS C:\Temp> .\New-CtmADKrbtgtKeys.ps1

This script can be used to perform a single reset of the krbtgt key that is shared by all
writable domain controllers in the domain in which it is run.

This script has 3 modes:
- Mode 1 is Informational Mode. This mode is safe to run at any time and makes no changes
to the environment. It will analyze the environment and check for issues that may impact
the successful execution of Mode 2 or Mode 3.
- Mode 2 is Simulation Mode. This mode will perform all the analysis and checks included
in Mode 1. It will also initiate a single object replication of the krbtgt object from
the PDC emulator DC to every writable domain controller that is reachable. This
replication is not to replicate changes (no changes will be made). Instead, this replication
is performed so that the replication time for mode 3 can be estimated.
- Mode 3 is Reset Mode. This mode will perform all the analysis and checks included
in Mode 1. It will also perform a single reset of the krbtgt key on the PDC emulator DC.
If the krbtgt reset is successful, it will automatically initiate a single object
replication of krbtgt from the PDC emulator DC to every writable domain controller that
is reachable. Once the replication is complete, the total impact time will be displayed.
During the impact duration of Mode 3 (estimated in Mode 2), the following impacts may
be observed:
- Kerberos PAC validation failures: Until the new krbtgt key is replicated to all
writable DCs in the domain, applications which attempt KDC PAC validation may
experience KDC PAC validation failures. This is possible when a client in one
site is accessing a Kerberos-authenticated application that is in a different site.
If that application is not a trusted part of the operating system, it may attempt
to validate the PAC of the client's Kerberos service ticket against the KDC (DC) in
its site. If the DC in its site does not yet have the new krbtgt key, this KDC PAC
validation will fail. This will likely manifest itself to the client as
authentication errors for that application. Once all DCs have the new krbtgt key,
some affected clients may recover gracefully and resume functioning normally. If not,
rebooting the affected client(s) will resolve the issue. This issue may not occur if
the replication of the new krbtgt key is timely and successful and no applications
attempt KDC PAC validation against an out of sync DC during that time.
- Kerberos TGS request failures: Until the new krbtgt key is replicated to all writable
DCs in the domain, a client may experience Kerberos authentication failures. This is
when a client in one site has obtained a Kerberos user ticket (TGT) from a DC that has
the new krbtgt, but then subsequently attempts to obtain a service ticket via a TGS
request against a DC in a different site. If that DC does not also have the new krbtgt
key, it will not be able to decrypt the client's TGT, which will result in a TGS
request failure. This will manifest itself to the client as authenticate errors.
However, it should be noted that this impact is very unlikely, because it is very
unlikely that a client will attempt to obtain a service ticket from a different DC
than the one from which their TGT was obtained, especially during the relatively short
impact duration of Mode 3.

It is highly recommended that Mode 1 be run first, then Mode 2, and then Mode 3.

In which mode do you wish to run the script?

1 --- Informational Mode (no changes made; no replication triggered)
2 --- Simulation Mode (no changes made, but replication WILL BE triggered for estimation purposes)
3 --- Reset Mode (krbtgt WILL BE reset once, and replication WILL BE triggered)
0 --- Exit

(Enter 1-3, or 0 to exit):
```



krbtgt Password Reset

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

```
Administrator: Windows PowerShell

In which mode do you wish to run the script?

 1 --- Informational Mode (no changes made; no replication triggered)
 2 --- Simulation Mode (no changes made, but replication WILL BE triggered for estimation purposes)
 3 --- Reset Mode (krbtgt WILL BE reset once, and replication WILL BE triggered)
 0 --- Exit

(Enter 1-3, or 0 to exit): 1
Checking for script pre-requisites...

Checking for ActiveDirectory Powershell module.....PASSED
Checking for GroupPolicy Powershell module.....PASSED
Checking if RPCPING.exe is installed and in the path.....PASSED
Checking if REPADMIN.exe is installed and in the path.....PASSED

Gathering and analyzing target domain information...

Domain NetBIOS name: DWP
Domain DNS name: dwp.de
PDC emulator: DC05.dwp.de
DomainMode: Windows2016Domain
Checking domain functional mode is 'Windows2008Domain' or higher.....PASSED

Gathering and analyzing krbtgt account information and domain Kerberos policy...

Krbtgt account: CN=krbtgt,CN=Users,DC=dwp,DC=de
Krbtgt account password last set on PDC emulator: 12/28/2018 2:29:03 PM
Kerberos maximum lifetime for user ticket (TGT lifetime): 10 hours
Kerberos maximum tolerance for computer clock synchronization: 5 minutes
Checking if all tickets based on the previous (N-1) krbtgt key have expired.....PASSED

Gathering and analyzing writable domain controller information...

Checking RPC connectivity to domain controllers:
Checking RPC connectivity to DC05.dwp.de .....PASSED
Checking RPC connectivity to DC01.dwp.de .....PASSED
Check for RPC connectivity to writable domain controllers PASSED: All writable DCs were reachable.

Logged to file: New-CtmADKrbtgtKeys_2019-07-03T11.49.12.0498433+02.00.log
PS C:\Temp>
```

Zu jedem Schritt wird ein Log geschrieben.

```
New-CtmADKrbtgtKeys_2019-07-03T11.49.12.0498433+02.00 - Notepad

File Edit Format View Help

ScriptMode           : 1
PreFlightPassed      : True
DomainModePassed     : True
NMinusOneTicketExpirationPassed : True
RpcToDCsPassed       : True

Windows (CRLF) Ln 1, Col 1 100%
```



krbtgt Password Reset

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

Die Replikation, RPC Konnektivität wurde überprüft.

```
Administrator: Windows PowerShell

(Enter 1-3, or 0 to exit): 2
Checking for script pre-requisites...

  Checking for ActiveDirectory Powershell module....PASSED
  Checking for GroupPolicy Powershell module....PASSED
  Checking if RPCPING.exe is installed and in the path....PASSED
  Checking if REPADMIN.exe is installed and in the path....PASSED

Gathering and analyzing target domain information...

  Domain NetBIOS name: DWP
  Domain DNS name: dwp.de
  PDC emulator: DC05.dwp.de
  DomainMode: Windows2016Domain
  Checking domain functional mode is 'Windows2008Domain' or higher....PASSED

Gathering and analyzing krbtgt account information and domain Kerberos policy...

  Krbtgt account: CN=krbtgt,CN=Users,DC=dwp,DC=de
  Krbtgt account password last set on PDC emulator: 12/28/2018 2:29:03 PM
  Kerberos maximum lifetime for user ticket (TGT lifetime): 10 hours
  Kerberos maximum tolerance for computer clock synchronization: 5 minutes
  Checking if all tickets based on the previous (N-1) krbtgt key have expired....PASSED

Gathering and analyzing writable domain controller information...

  Checking RPC connectivity to domain controllers:
    Checking RPC connectivity to DC05.dwp.de ....PASSED
    Checking RPC connectivity to DC01.dwp.de ....PASSED
  Check for RPC connectivity to writable domain controllers PASSED: All writable DCs were reachable.

Replicating krbtgt object to all writable domain controllers that are reachable...
  The krbtgt object replication WILL BE triggered if you proceed. Are you sure you wish to proceed?
  (Enter 'Y' to proceed or any other key to exit): y
  Replication of krbtgt from DC05.dwp.de to DC01.dwp.de ...SUCCEEDED Time: 00:00:00.0828798

The total duration of impact when running Mode 3 will be approximately: 00:00:00.1141733
Logged to file: New-CtmADKrbtgtKeys_2019-07-03T11.50.50.7709071+02.00.log
PS C:\Temp>
```

Das dazugehörige Log.

```
New-CtmADKrbtgtKeys_2019-07-03T11.50.50.7709071+02.00 - Notepad

File Edit Format View Help

ScriptMode           : 2
PreFlightPassed      : True
DomainModePassed     : True
NMinusOneTicketExpirationPassed : True
RpcToDCsPassed       : True
ReplicationCheckSucceeded : True
ImpactDurationEstimate : 00:00:00.1141733

Windows (CRLF) Ln 1, Col 1 100%
```



krbtgt Password Reset

Die Passwortänderung führen wir mit Schritt 3 durch.

Das Passwort wurde geändert und repliziert.

```
Administrator: Windows PowerShell
(Enter 1-3, or 0 to exit): 3
Checking for script pre-requisites...

Checking for ActiveDirectory Powershell module....PASSED
Checking for GroupPolicy Powershell module....PASSED
Checking if RPCPING.exe is installed and in the path....PASSED
Checking if REPADMIN.exe is installed and in the path....PASSED

Gathering and analyzing target domain information...

Domain NetBIOS name: DWP
Domain DNS name: dwp.de
PDC emulator: DC05.dwp.de
DomainMode: Windows2016Domain
Checking domain functional mode is 'Windows2008Domain' or higher....PASSED

Gathering and analyzing krbtgt account information and domain Kerberos policy...

Krbtgt account: CN=krbtgt,CN=Users,DC=dwp,DC=de
Krbtgt account password last set on PDC emulator: 12/28/2018 2:29:03 PM
Kerberos maximum lifetime for user ticket (TGT lifetime): 10 hours
Kerberos maximum tolerance for computer clock synchronization: 5 minutes
Checking if all tickets based on the previous (N-1) krbtgt key have expired....PASSED

Gathering and analyzing writable domain controller information...

Checking RPC connectivity to domain controllers:
Checking RPC connectivity to DC05.dwp.de ....PASSED
Checking RPC connectivity to DC01.dwp.de ....PASSED
Check for RPC connectivity to writable domain controllers PASSED: All writable DCs were reachable.

Replicating krbtgt object to all writable domain controllers that are reachable...
Replication of krbtgt from DC05.dwp.de to DC01.dwp.de ...SUCCEEDED Time: 00:00:00.0468660

The total duration of impact when running Mode 3 will be approximately: 00:00:00.0468660
Resetting krbtgt key and replicating krbtgt object to all reachable domain controllers...

WARNING!!! The krbtgt key WILL BE reset AND krbtgt object replication WILL BE triggered if you proceed. Are you sure
you wish to proceed?
If you proceed, the impact duration of Mode 3 (described above) will begin and not end until all DCs obtained the new
krbtgt key.
(Enter 'Y' to proceed or any other key to exit): y

Resetting krbtgt key....SUCCEEDED

Replication of krbtgt from DC05.dwp.de to DC01.dwp.de ...SUCCEEDED Time: 00:00:00.0312643
The total duration of impact when running mode 3 was: 00:00:00.3124955

Validating krbtgt password last set is in sync with PDC emulator...
PDC emulator: Krbtgt account password last set on DC05.dwp.de ....7/3/2019 12:30:18 PM
Checking krbtgt account password last set on DC01.dwp.de ....PASSED Last set: 7/3/2019 12:30:18 PM

Check if krbtgt key on all writable domain controllers was in sync with PDC emulator PASSED. All reachable DCs were i
n sync with the PDC emulator..

Logged to file: New-CtmADKrbtgtKeys_2019-07-03T12.29.51.7933228+02.00.log
PS C:\Temp>
```

Auch hier ein Log:

```
New-CtmADKrbtgtKeys_2019-07-03T12.29.51.7933228+02.00 - Notepad
File Edit Format View Help

ScriptMode : 3
PreFlightPassed : True
DomainModePassed : True
NMinusOneTicketExpirationPassed : True
RpcToDCsPassed : True
ReplicationCheckSucceeded : True
ImpactDurationEstimate : 00:00:00.0468660
ResetSucceeded : True
PostResetReplicationSucceeded : True
ImpactDuration : 00:00:00.3124955
NewKrbtgtKeyReplValidationPassed : True

Windows (CRLF) Ln 1, Col 1 100%
```



krbtgt Password Reset

Überprüfe das Ganze auf dem 2. DC.

Die Änderung wurde sauber repliziert.

| Attribute | Value |
|-----------------------|--|
| lastLogoff | (never) |
| lastLogon | (never) |
| logonCount | 0 |
| msDS-SupportedEncr... | 0x0 = () |
| name | krbtgt |
| objectCategory | CN=Person,CN=Schema,CN=Configuration,... |
| objectClass | top; person; organizationalPerson; user |
| objectGUID | 44d30e0c-a0ce-478d-91e6-79e37d6ec8d0 |
| objectSid | S-1-5-21-796728725-704351489-224380805 |
| primaryGroupID | 513 = (GROUP_RID_USERS) |
| pwdLastSet | 7/3/2019 12:30:18 PM W. Europe Daylight |
| replPropertyMetaData | AttID Ver Loc.USN Org.DSA |
| sAMAccountName | krbtgt |
| sAMAccountType | 805306368 = (NORMAL USER ACCOUNT) |

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.

```
55 Catch [System.Exception]
56 {
57     If ($Error.FullyQualifiedErrorId -eq 'Comma' Write-Host -ForegroundColor Red "The 'RPCPING.exe' utility is not available. Ins
58     Write-Host -ForegroundColor Red "An unknown attempt to execute 'RPCPING.exe'... exiting."; Exit
59 }
60
61 # Check output of RPCPING for success
62 If ($RpcPingResult -like "abgeschlossen") {Return (New-Object -TypeName PSObject -Property @{'Success'=$true; 'Message'="$Hostname - RPC connectivit
63 }
64 # Check output of RPCPING for exceptions
65 If ($RpcPingResult -like "Exception 5") {Return (New-Object -TypeName PSObject -Property @{'Success'=$false; 'Message'="$Hostname - Access is den
66 If ($RpcPingResult -like "Exception 1722") {Return (New-Object -TypeName PSObject -Property @{'Success'=$false; 'Message'="$Hostname - RPC server un
67 If ($RpcPingResult -like "Exception") {Return (New-Object -TypeName PSObject -Property @{'Success'=$false; 'Message'="$Hostname - RPC to the ta
68 }
69
70 function Start-CtmADSingleObjectReplication
```



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)
```