Kerberos Token Size

Die maximale Kerberos Token Size liegt Default bei den aufgelisteten Systemen:

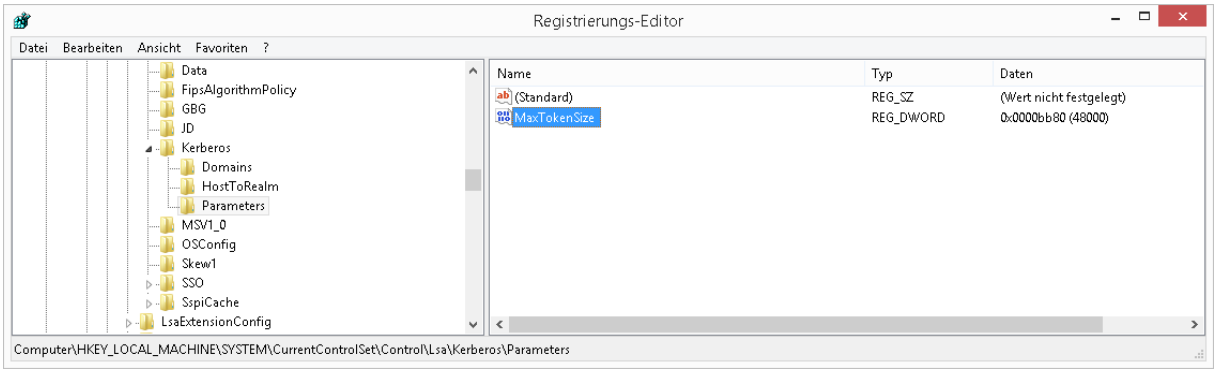
12 KB = Windows 7 und Server 2008R2

48 KB = Windows 8, Server 2012 und Server 2016

Die Token Size kann in der Registry durch einen neu zu erstellenden DWORD-Wert (32-Bit) angepasst werden.

Dazu navigieren wir zu und erstellen einen neuen Wert (MaxTokenSize) Dezimal 48000.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\



Diese Vorgehensweise behebt das Problem der Anmeldung an einen Server oder Client.

MaxTokenSize definiert hierbei den Empfangspuffer für die Antworten vom KDC (Key Distribution Center / Kerberos Server) über direkte und vererbte Gruppenmitgliedschaften.

Aus diesem Puffer wiederum bezieht LSASS (Local Security Authority Subsystem Service) über den Kerberos Client die Ticket Informationen für den entsprechenden User- oder Computer Kontext.

Passt die Antwort des KDC nicht in den Puffer, kann LSASS das entsprechende Ticket auch nicht für einen Ressourcenzugriff (z.B. File Server) zur Verfügung stellen.

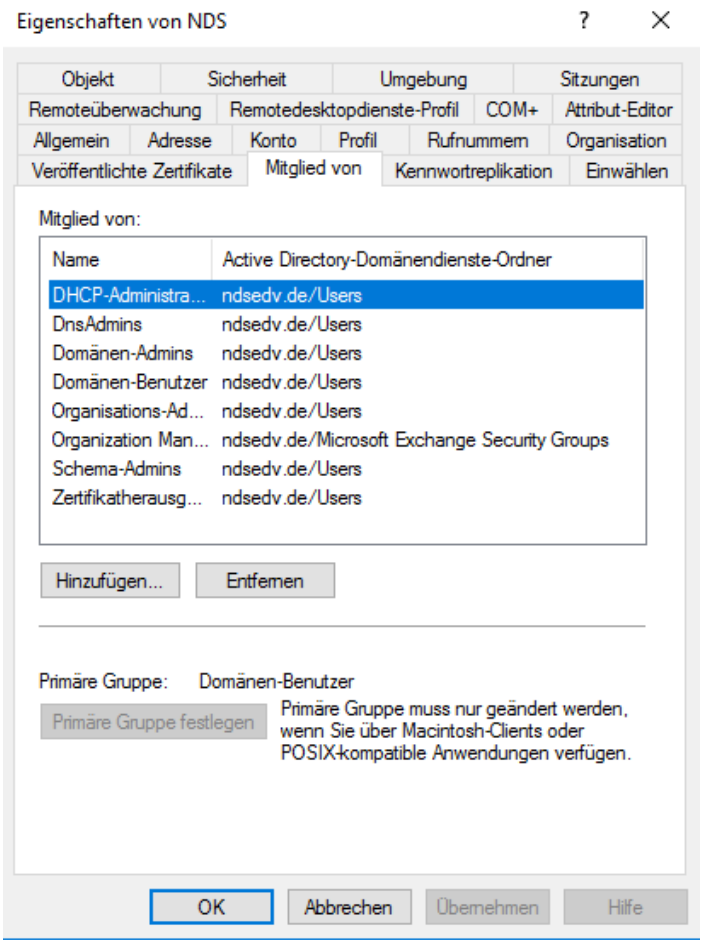
Der Empfangspuffer hat eine definierte Struktur, es ist kein flacher Speicherbereich, bei dem intern schon von einem Token gesprochen werden kann. Diese Struktur ist dafür verantwortlich, dass man MaxTokenSize nicht auf das Byte genau berechnen kann. Daher ist das Vorgehen zur Bestimmung von MaxTokenSize, in einem Microsoft Artikel sehr gut beschrieben.

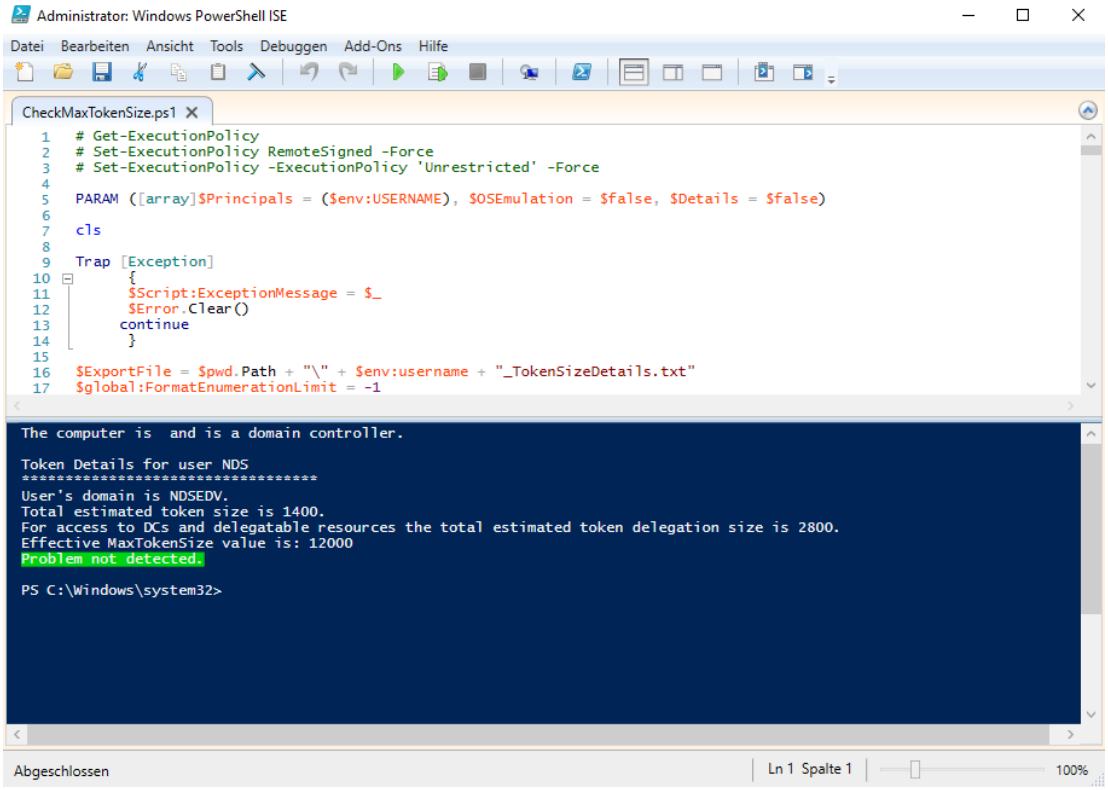
https://support.microsoft.com/en-us/kb/327825
https://support.microsoft.com/en-us/kb/938118
https://support.microsoft.com/en-us/kb/313661

Erstellt von Jörn Walter www.der-windows-papst.de – 30.11.2016

Kerberos Token Size

Die aktuelle Token Size kann mithilfe eines Powershell Skripts ermittelt werden.

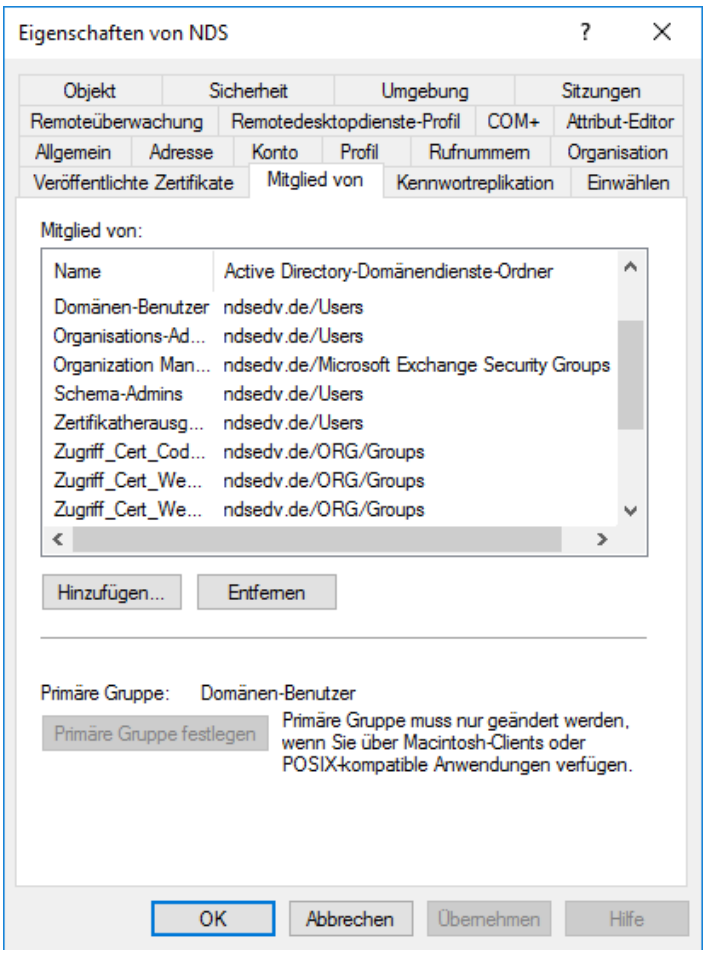




Erstellt von Jörn Walter www.der-windows-papst.de – 30.11.2016

Kerberos Token Size

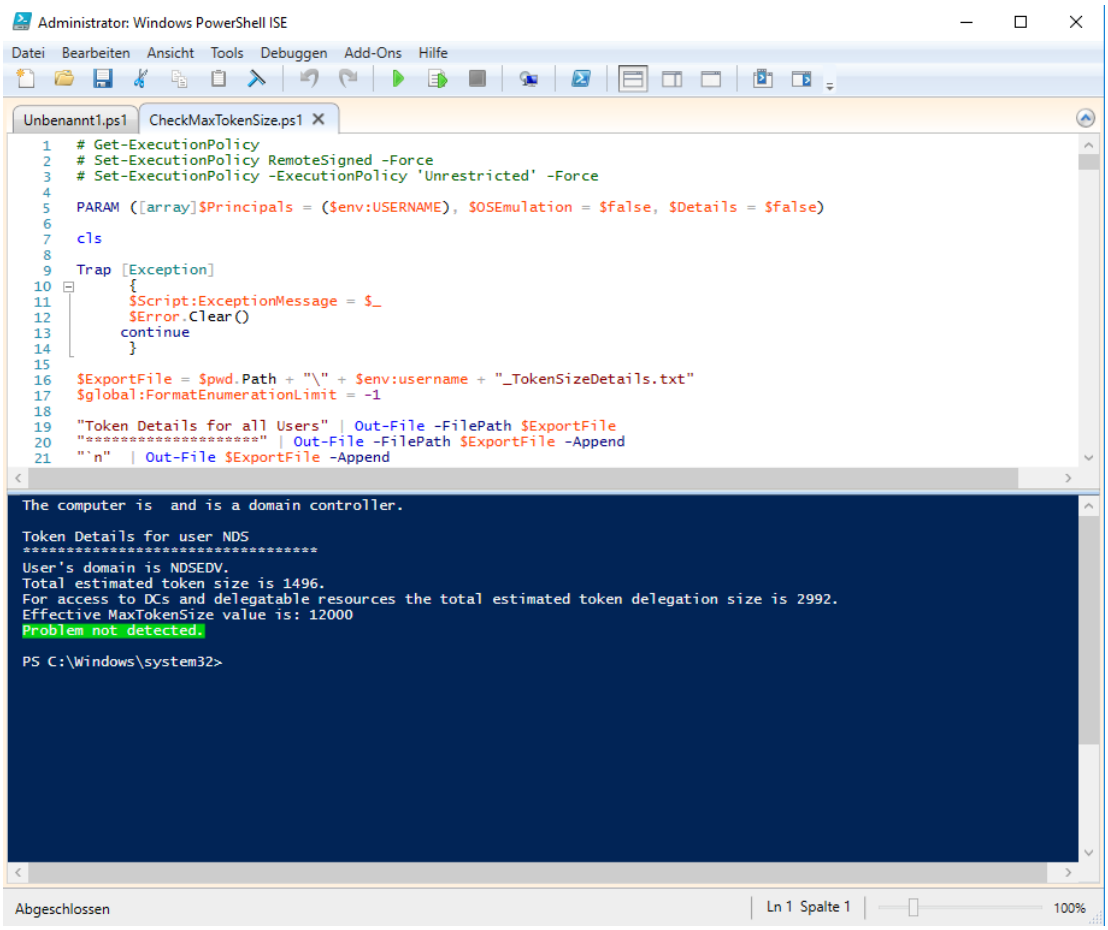
Wenn ich den User NDS in 8 weitere globale Security Groups hinzufüge erhöht sich auch ersichtlich die Größe des Tokens um weitere 96 Byte. Jede weitere Gruppenmitgliedschaft erhöht das Token um 12 Byte.



Die Größe liegt nun bei 1496 Byte. Wäre das Token (SID Informationen) z.B. 10699 Byte groß würde dieser schon nicht mehr in den Default Puffer von 12000 Byte passen. Die Größe des Tokens wird nicht nur durch die Gruppenmitgliedschaften bestimmt, sondern es fließen noch weitere Informationen mit ein die das Token zusätzlich aufblähen.

https://gallery.technet.microsoft.com/scriptcenter/Check-for-MaxTokenSize-520e51e5

Kerberos Token Size



Gibt es Authentifizierungsprobleme bei der Nutzung bereitgestellter Services z.B. über einen IIS, dann muss die maximale Größe des HTTP Headers angepasst werden.

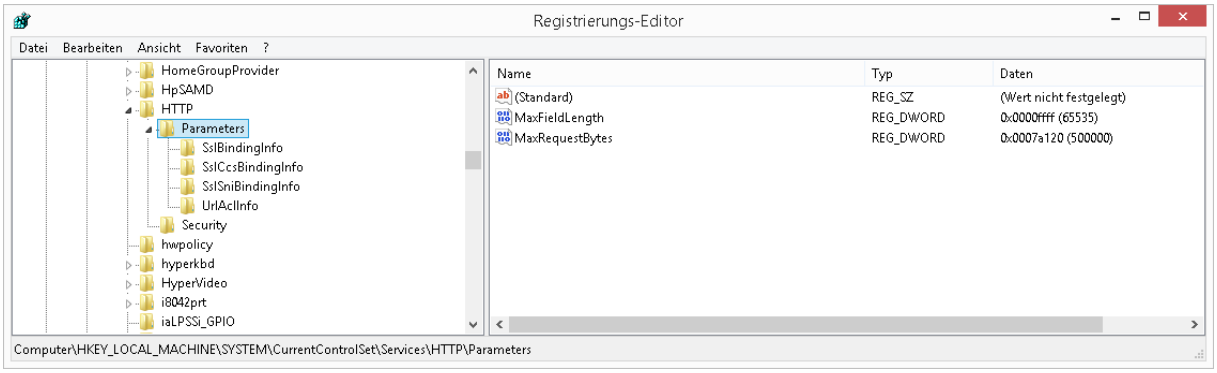
Die Fehlermeldung lautet in der Regel „Bad Request (Request Header Too Long).

IIS Base64-Kodierung > Der HTTP HEADER fasst max. 48KB. Bei einer Kerberos Delegation wird das Token doppelt so groß berechnet. Ist das Token des Users 8200 KB groß *2 durch die Kerberos Delegation kommen wir auf 16400 KB.

Gehen wir davon aus, dass der User eine TokenSize von 16400 Byte hat. Der GET Request eines IIS fasst Default aber nur 16K, die Authentifizierung schlägt fehl.

Um dieses Problem zu lösen müssen weitere Werte in der Registry erstellt werden.

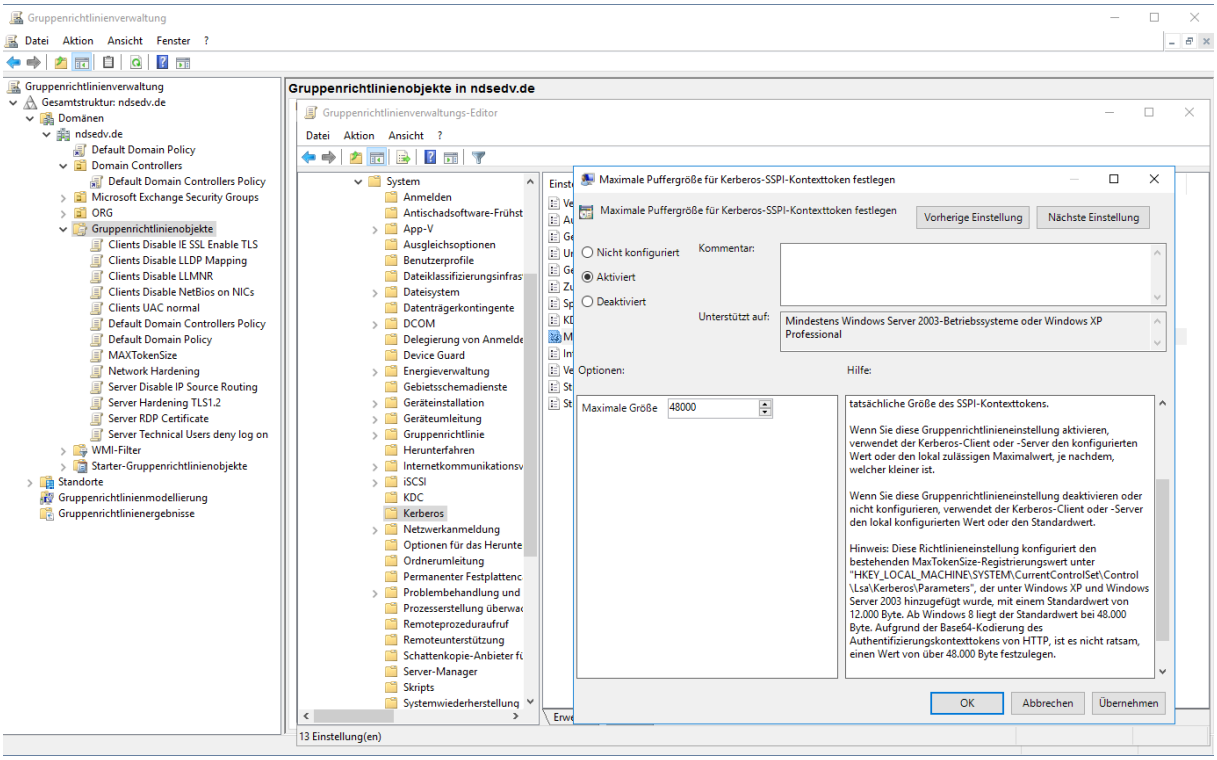
Dazu navigieren wir zu und erstellen 2 neue DWORD-Wert (32-Bit).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters]

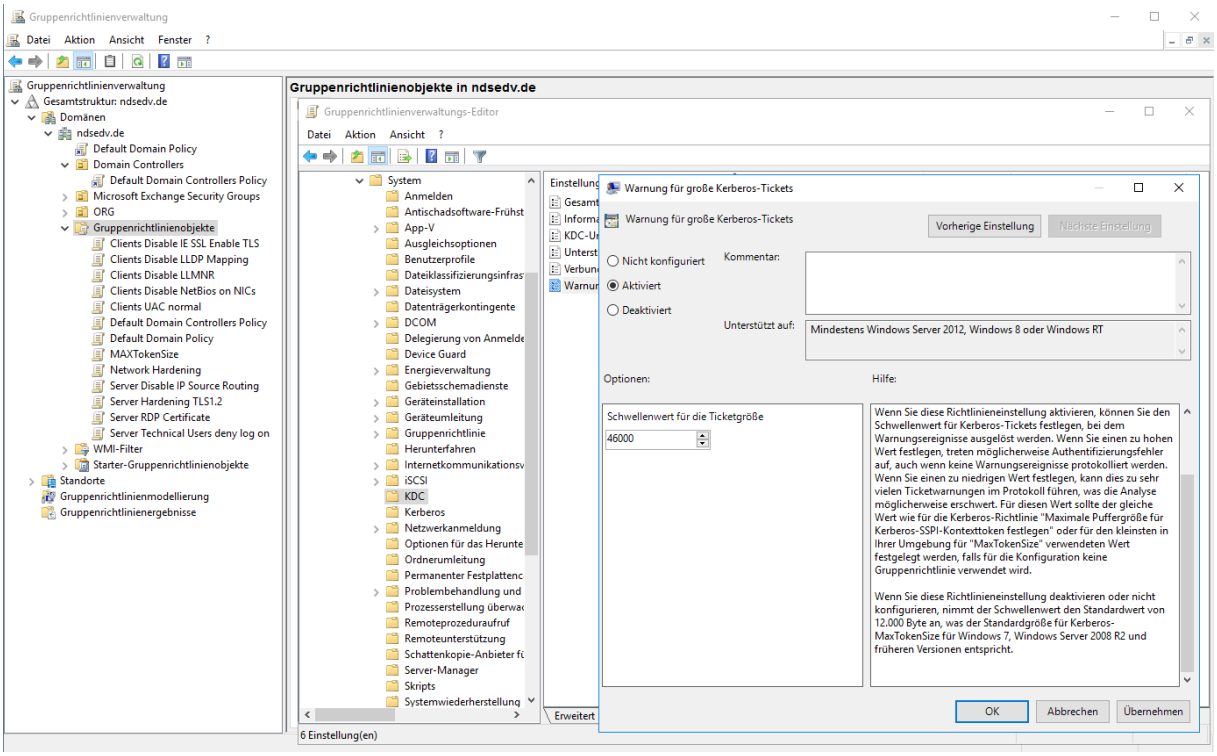


Kerberos Token Size

Damit der gesamte Forest konsistent bleibt, sollten die Anpassungen auf allen Servern, Clients und Domain Controller vorgenommen werden.

Die Umsetzung würde ich wie gehabt über eine Gruppenrichtlinie vornehmen. Ein Hinweis am Rande. Bei dieser Einstellung handelt es sich nicht um eine echte Richtlinie, sondern um eine Preferences. Der Unterschied liegt darin, das eine Preferences nicht zurückgezogen werden kann, wie das z.B. bei einer Policy der Fall wäre. Ist der Registry Wert erst einmal ausgerollt bleibt dieser bei Rückzug der Richtlinie erhalten.

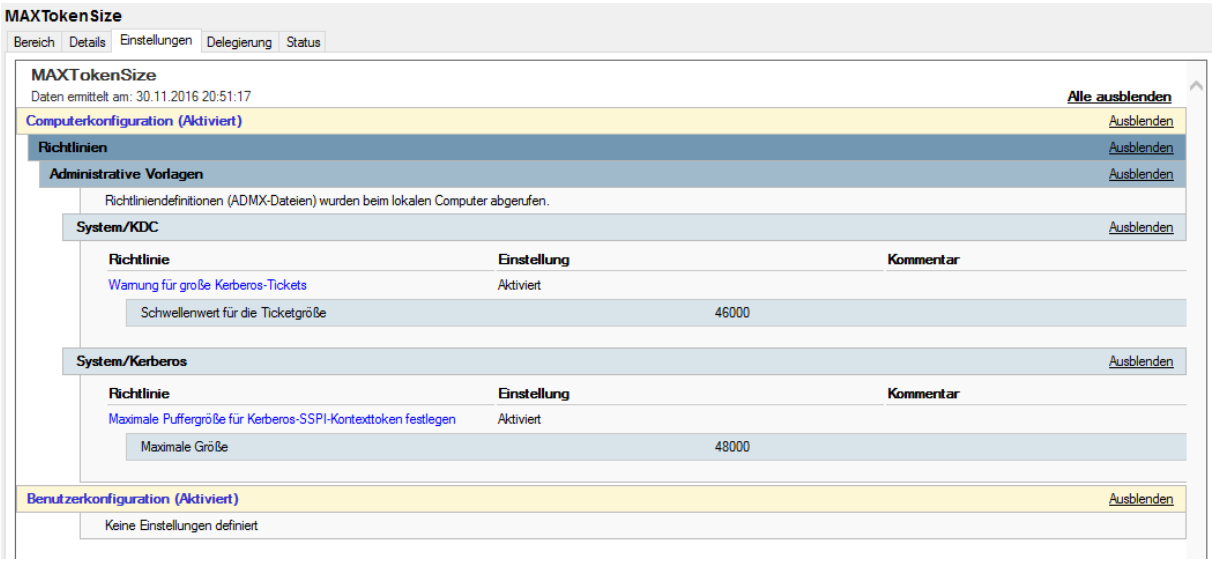




Event ID 31 > Kerberos -Key-Distribution-Center

Kerberos Token Size

HTML Bericht:



Kerberos Funktion vereinfachte Darstellung

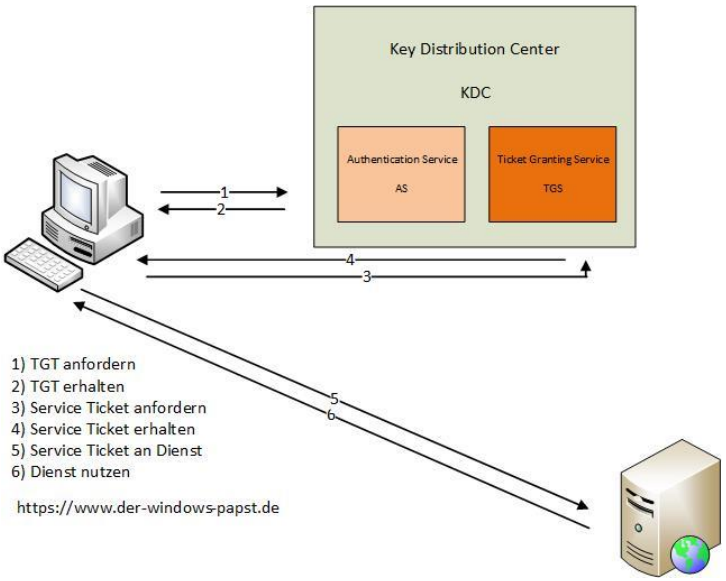
Für den Zugriff auf einen Service benötigen wir ein Ticket.

Für den Erhalt eines Tickets müssen wir uns am Authentication Server authentifizieren. Der AS erstellt daraufhin einen Session Key und einen Verschlüsselungs-Schlüssel, der auf unserem Passwort und einer zufälligen Zeichenfolge basiert. Der Session Key ist quasi ein Ticket für das Ticket.

Den Session Key schickt der Client an den Ticket-Granting-Server (TGS). Der TGS liefert anschließend das eigentliche Ticket

Der zu kontaktierende Service nimmt das Ticket an oder lehnt es ab. Bei Annahme kann der Nutzer auf den entsprechenden Service zugreifen.

Das Ticket hat einen Zeitstempel und eine Gültigkeit. Solange die vorgegebene Gültigkeit nicht abläuft, kann der Nutzer weitere Services über dieses Ticket nutzen, ohne dass er sich erneut am AS und TGS authentifizieren muss.



Kerberos Token Size

Ein Kerberos Ticket enthält kryptografische Informationen zur Authentizitätskontrolle der Kommunikationspartner somit ist dieses eine Art digitaler Ausweis.

Übersicht der Default Werte sortiert nach Betriebssystemen:

OS	Default Size
Windows 2000	8,000 bytes
Windows 2000 SP2	12,000 bytes
Windows 2003	12,000 bytes
Windows XP	12,000 bytes
Windows Vista	12,000 bytes
Windows 7	12,000 bytes
Windows 2008	12,000 bytes
Windows 2008 R2	12,000 bytes
Windows 8	48,000 bytes
Windows 2012	48,000 bytes
Windows 8.1	48,000 bytes
Windows 2012 R2	48,000 bytes
Windows 2016	48,000 bytes

Powershell Skript:

CheckMaxTokenSize.txt

Registry Einträge:

HTTP Header:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters]
"MaxFieldLength"=dword:0000ffff
"MaxRequestBytes"=dword:0007a120
```

MaxTokenSize:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"MaxTokenSize"=dword:00048000
```

Fehlermeldungen Event Viewer:

SQL Server ID 40960
Remote Desktop ID 6

Token Größen:

Eine lokale Domänen Gruppe fasst 40 Byte
Eine Sicherheits- und universelle Gruppe 8 Byte
Token Grundgröße ~1200 Byte

Maximal sind 1015 Gruppen möglich.

Erstellt von Jörn Walter www.der-windows-papst.de – 30.11.2016