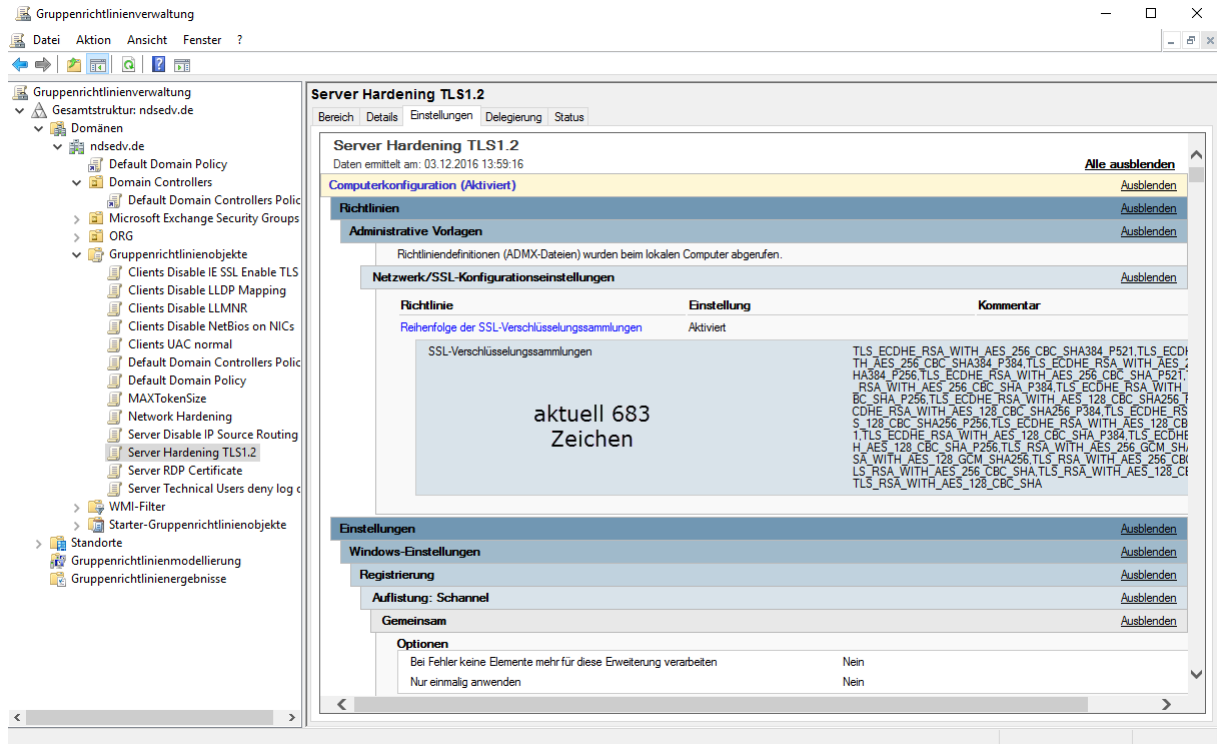


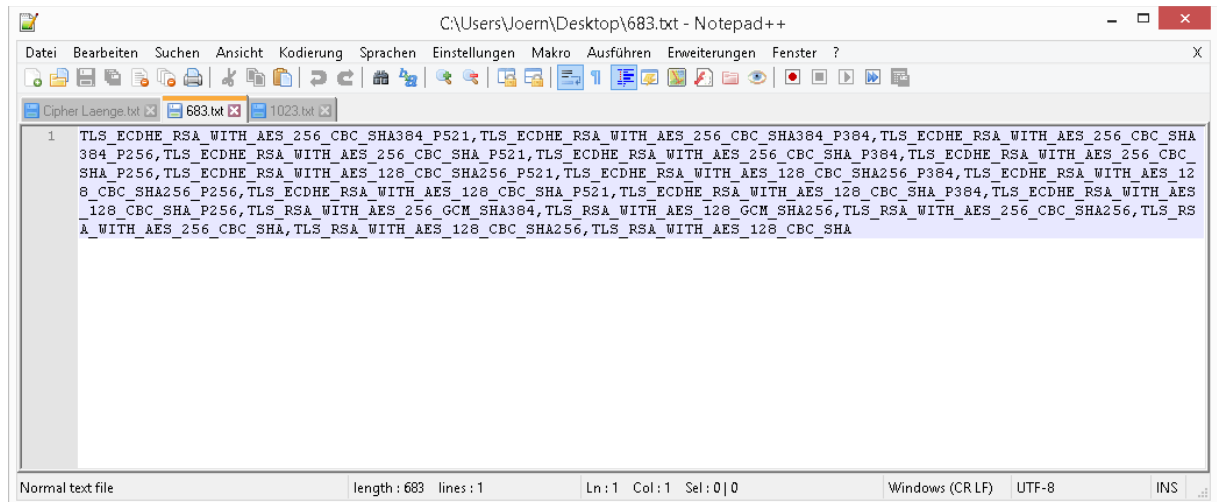
# Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

Ein Textfeld in den Administrativen Vorlagen welches Werte in die REG\_SZ schreibt ist auf 1023 Zeichen begrenzt. Dieses Problem bekam ich bei der Umstellung auf TLS1.2. Ich experimentierte in meiner Testumgebung und wunderte mich immer wieder darüber das ein Teil der Ciphers fehlte. Die Lösung möchte ich niemanden vorenthalten.

Dieses Beispiel zeigt eine Suite mit 683 Zeichen, alles Ok.

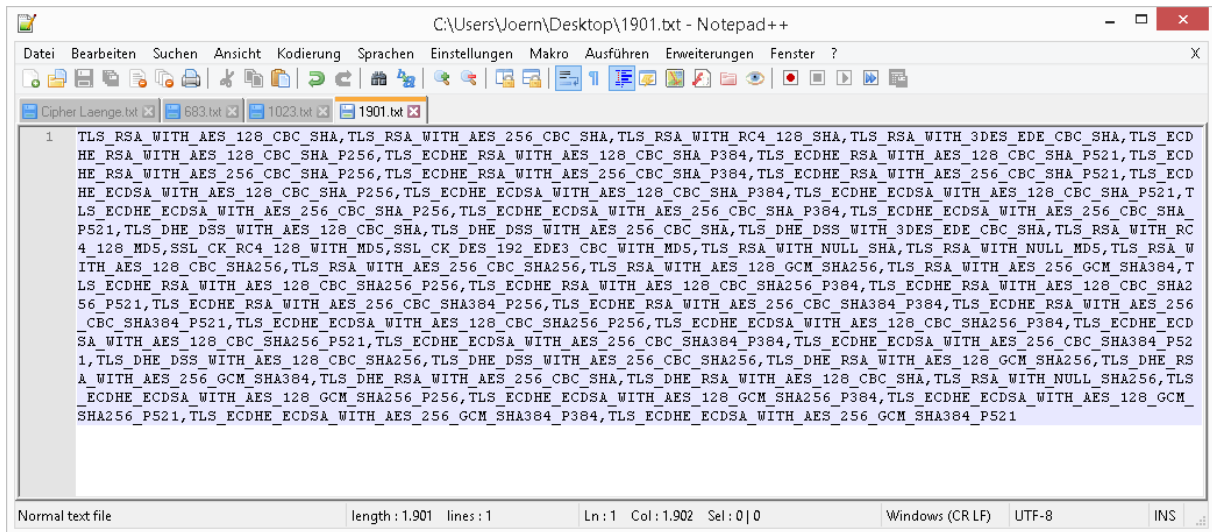


Die gezählten Zeichen in Notepad++

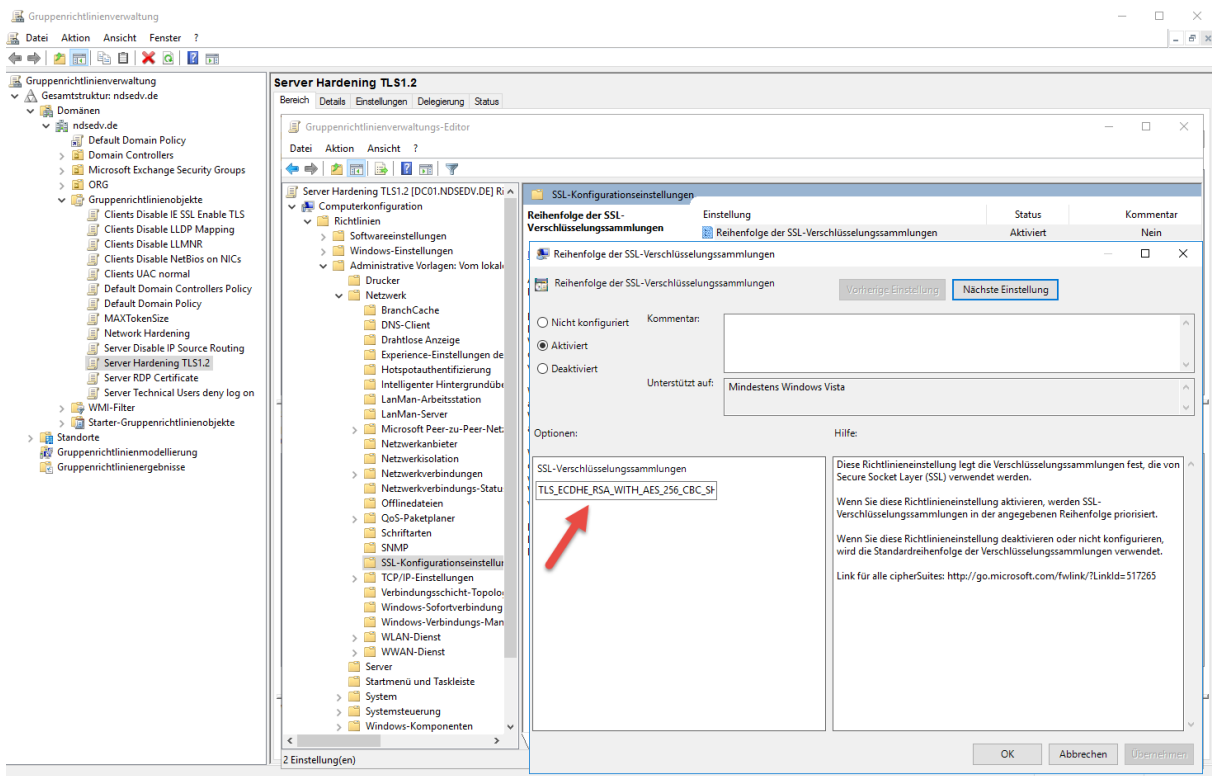


# Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

Jetzt füge ich eine Suite mit 1901 Zeichen in das Textfeld ein.



## Copy & Paste



# Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

So sah das Ergebnis dann aus. Die Suite endete mit den Buchstaben AE

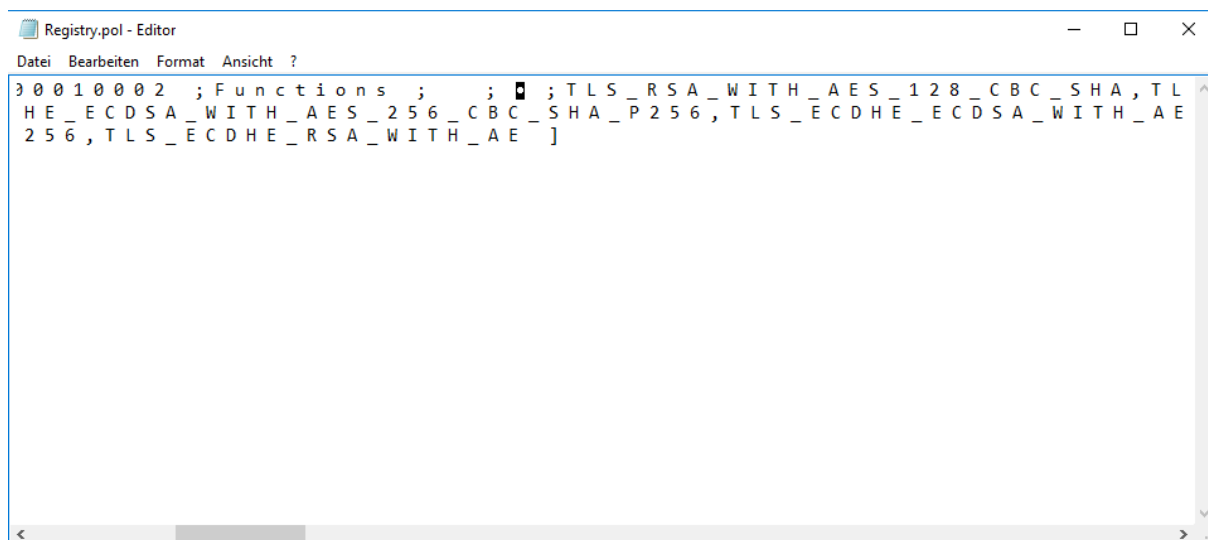
The screenshot shows the Group Policy Editor window for 'Server Hardening TLS1.2'. The left-hand navigation pane is expanded to show the hierarchy: Domänen > ndsevd.de > Gruppenrichtlinienobjekte > Server Hardening TLS1.2. The main window displays the configuration for this policy, which is currently set to 'Aktiviert'. Under the 'Netzwerk/SSL-Konfigurationseinstellungen' section, a list of cipher suites is shown, including TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, and various ECDHE and ECDSA variants.

Hier der Beweis das es sich um 1023 Zeichen handelt.

The screenshot shows a Notepad++ window with the file '1023.txt' open. The text content is a single line of cipher suite strings, which has been highlighted in blue. The status bar at the bottom of the window shows 'length: 1.023 lines: 1', confirming the exact character count of the text.

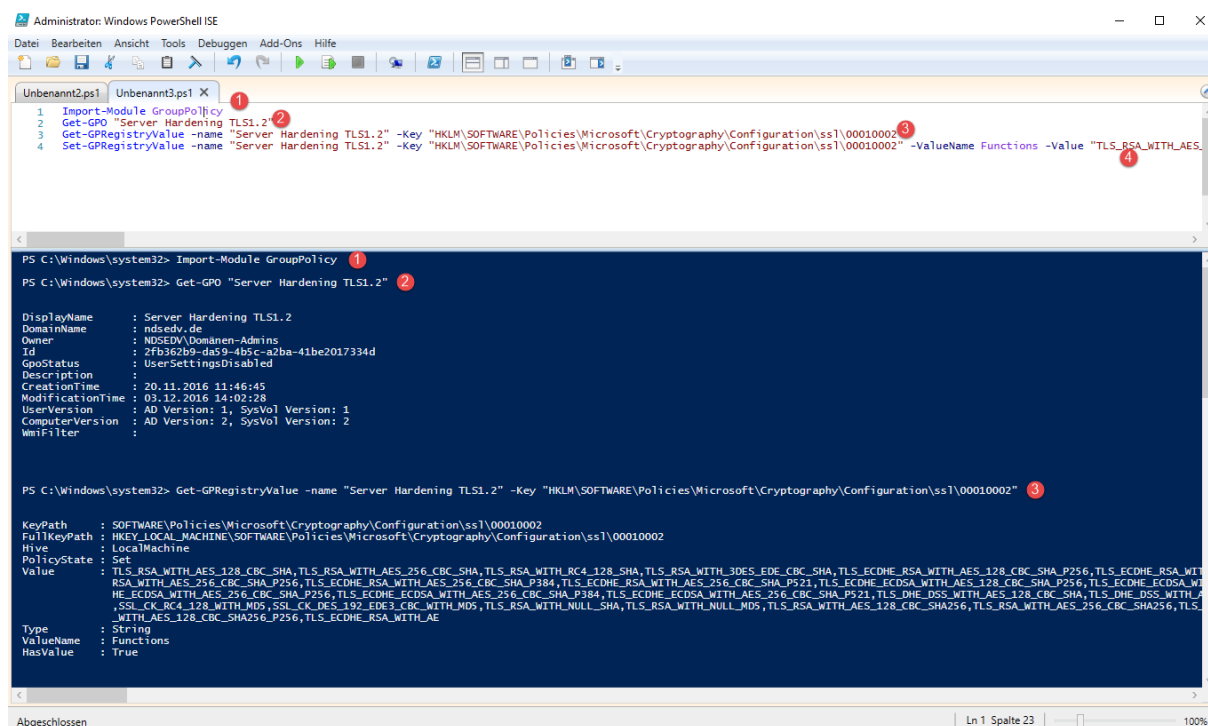
## Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

In der Registry.pol das gleiche Ergebnis.



```
3 0010002 ; Functions ; ; TLS_RSA_WITH_AES_128_CBC_SHA, TL
HE_ECDSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AE
256, TLS_ECDHE_RSA_WITH_AE ]
```

Also musste mal wieder die Powershell aushelfen um das Problem zu lösen.



```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt2.ps1 Unbenannt3.ps1 X
1 Import-Module GroupPolicy
2 Get-GPO "Server Hardening TLS1.2"
3 Get-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002"
4 Set-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002" -ValueName Functions -Value "TLS_RSA_WITH_AES..."

PS C:\Windows\system32> Import-Module GroupPolicy
PS C:\Windows\system32> Get-GPO "Server Hardening TLS1.2"

DisplayName : Server Hardening TLS1.2
DomainName : ndsedv.de
Owner : NSEDEV\Domänen-Admins
Id : 2Fb362b9-da59-4b5c-a2ba-41be2017334d
GpoStatus : UserSettingsDisabled
Description :
CreationTime : 20.11.2016 11:46:45
ModificationTime : 03.12.2016 14:02:28
UserVersion : AD Version: 1, SysVol Version: 1
ComputerVersion : AD Version: 2, SysVol Version: 2
WmiFilter :

PS C:\Windows\system32> Get-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002"

KeyPath : SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002
FullKeyPath : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002
Hive : LocalMachine
PolicyState : Set
Value : TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA_P256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA_P384, TLS_DHE_DSS_WITH_AES_256_CBC_SHA_P521, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_256_GCM_SHA256

Type : String
ValueName : Functions
HasValue : True

Abgeschlossen Ln 1 Spalte 23 100%
```

Punkt 1 aktiviert das Module für die Gruppenrichtlinien

Punkt 2 liest die Informationen der Gruppenrichtlinie „Server Hardening TLS1.2“ aus.

Punkt 3 liest den Wert des aktuellen Schlüssels aus. Auch hier sehen wir das die Suite mit den Buchstaben AE endet.

# Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

Punkt 4 schreibt die Suite mit 1901 Zeichen in die Gruppenrichtlinie.

```
1 Import-Module GroupPolicy
2 Get-GPO "Server Hardening TLS1.2"
3 Get-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002"
4 Set-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002" -ValueName Functions -Value "TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_256_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256_P521, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384_P521, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521"
```

```
PS C:\Windows\system32> Set-GPRegistryValue -name "Server Hardening TLS1.2" -Key "HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002" -ValueName Functions -Value "TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_256_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256_P521, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384_P521, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521"
```

Hier nun das Ergebnis in der Detailansicht der Gruppenrichtlinie.

The screenshot shows the Group Policy Management console for the 'Server Hardening TLS1.2' policy. The left pane shows the hierarchy: Gruppenrichtlinienverwaltung > Gesamtstruktur: ndse.dv > Domänen > ndse.dv > Server Hardening TLS1.2. The main pane displays the policy details, including the name 'Server Hardening TLS1.2', the date it was last modified (03.12.2016 21:10:11), and the category 'Computerkonfiguration (Aktiviert)'. The 'Richtlinien' section shows 'Administrative Vorlagen' and 'Netzwerk/SSL-Konfigurationseinstellungen'. The 'Einstellungen' section shows 'Auflistung: Schannel' with 'Gemeinsam' set to 'Aktiviert'. The 'Options' section shows 'Bei Fehler keine Elemente mehr für diese Erweiterung verarbeiten' and 'Nur einmalig anwenden', both set to 'Nein'. The 'Registrierungselement: Event Logging' is also visible.

## Gruppenrichtlinien Editor 1023 Zeichen Textfeld Begrenzung

### Powershell Befehle:

```
Import-Module GroupPolicy
```

```
Get-GPO "Server Hardening TLS1.2"
```

```
Get-GPRegistryValue -name "Server Hardening TLS1.2" -Key  
"HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002"
```

1901 Zeichen:

```
Set-GPRegistryValue -name "Server Hardening TLS1.2" -Key  
"HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\ssl\00010002" -  
ValueName Functions -Value  
"TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WI  
TH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_  
128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RS  
A_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,T  
LS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CB  
C_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_  
WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,T  
LS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_25  
6_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_  
WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WI  
TH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5  
,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_SHA,TLS_RSA_WITH_  
NULL_MD5,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA  
256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,T  
LS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128  
_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE  
_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA  
384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_ECDSA_W  
ITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P  
384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_ECDSA_WITH  
_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521  
,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SH  
A256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GC  
M_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_C  
BC_SHA,TLS_RSA_WITH_NULL_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA  
256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,TLS_ECDHE_ECDSA  
_WITH_AES_128_GCM_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA3  
84_P384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521" -Type String
```