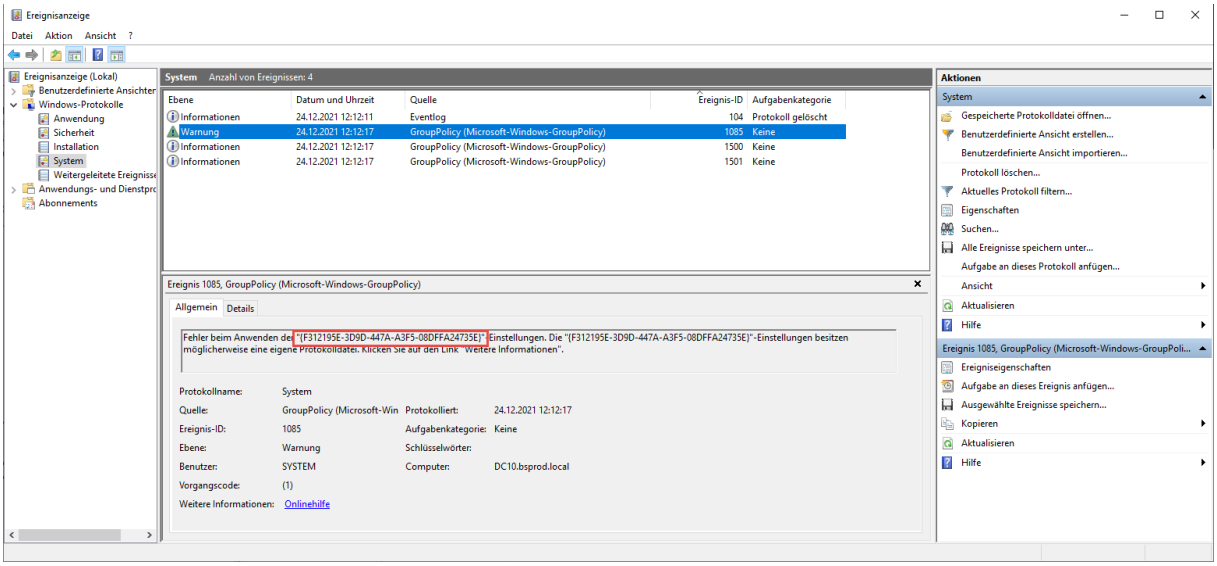
{F312195E-3D9D-447A-A3F5-08DFFA24735E}

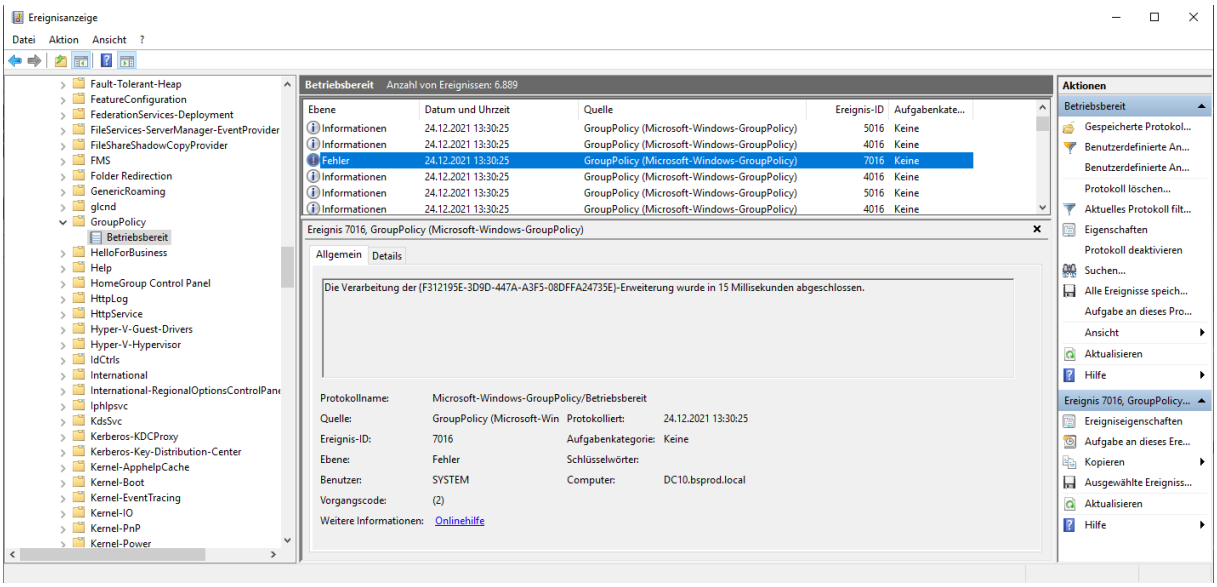
Eine Gruppenrichtlinie lässt sich nicht verarbeiten und im Ereignisprotokoll unter SYSTEM finden wir eine Warnung mit der Ereignis-ID 1085.

„Fehler beim Anwenden der Einstellungen. Die Einstellungen besitzen möglicherweise eine eigene Protokolldatei.“

Dieser Fehler kommt in der Regel dann zustande, wenn versucht wird etwas zu starten was es nicht gibt, oder mit einem falschen Wert konfiguriert ist; der nicht interpretiert werden kann.

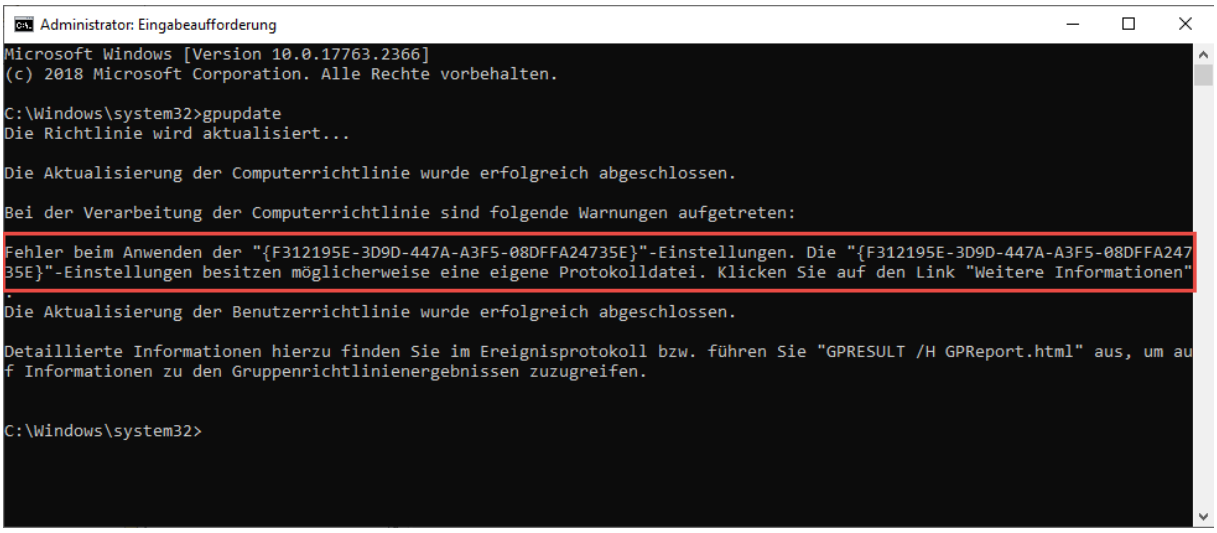


Parallel unter den Anwendungs- und Dienstprotokollen sehen wir einen Fehler bezogen auf die obere Warnung mit der Ereignis-ID 7016.

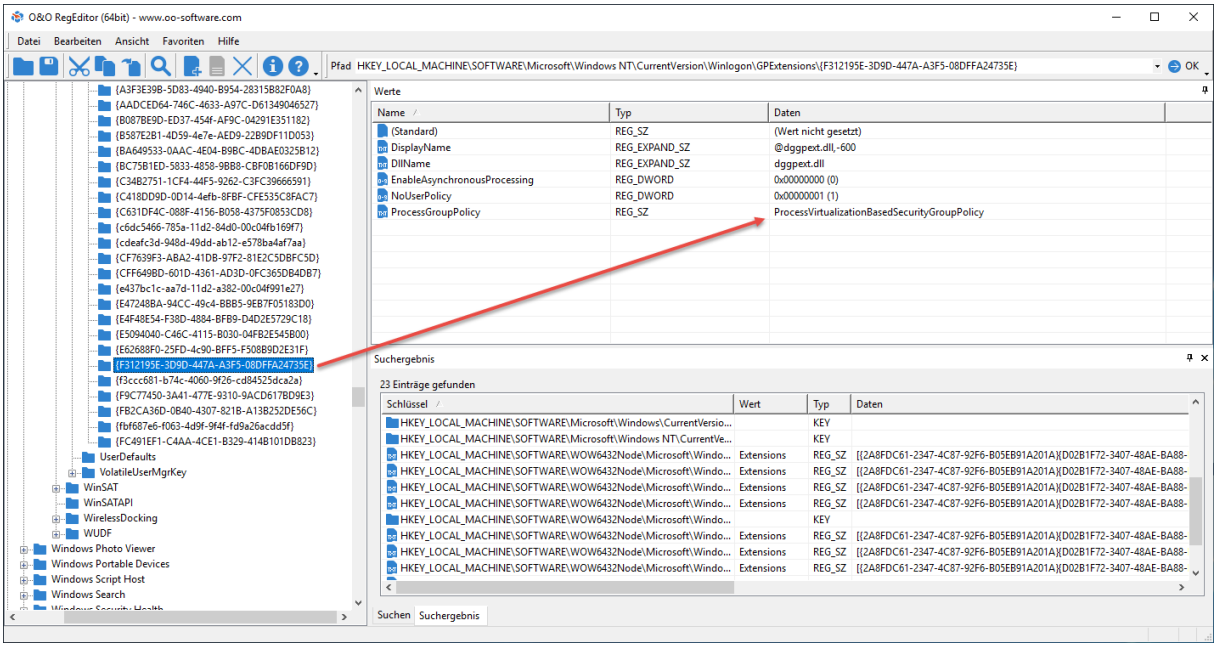


{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Ein manuell ausgeführtes GPUPDATE zeigt den Fehler ebenfalls noch einmal an.



Mithilfe eines Reg-Editors suche ich aus dem Fehlerprotokoll nach der GUID {F312195E-3D9D-447A-A3F5-08DFFA24735E}. Die GUID verweist auf die CSE VirtualizationBasedSecurity GPO (DeviceGuard / CredentialGuard)

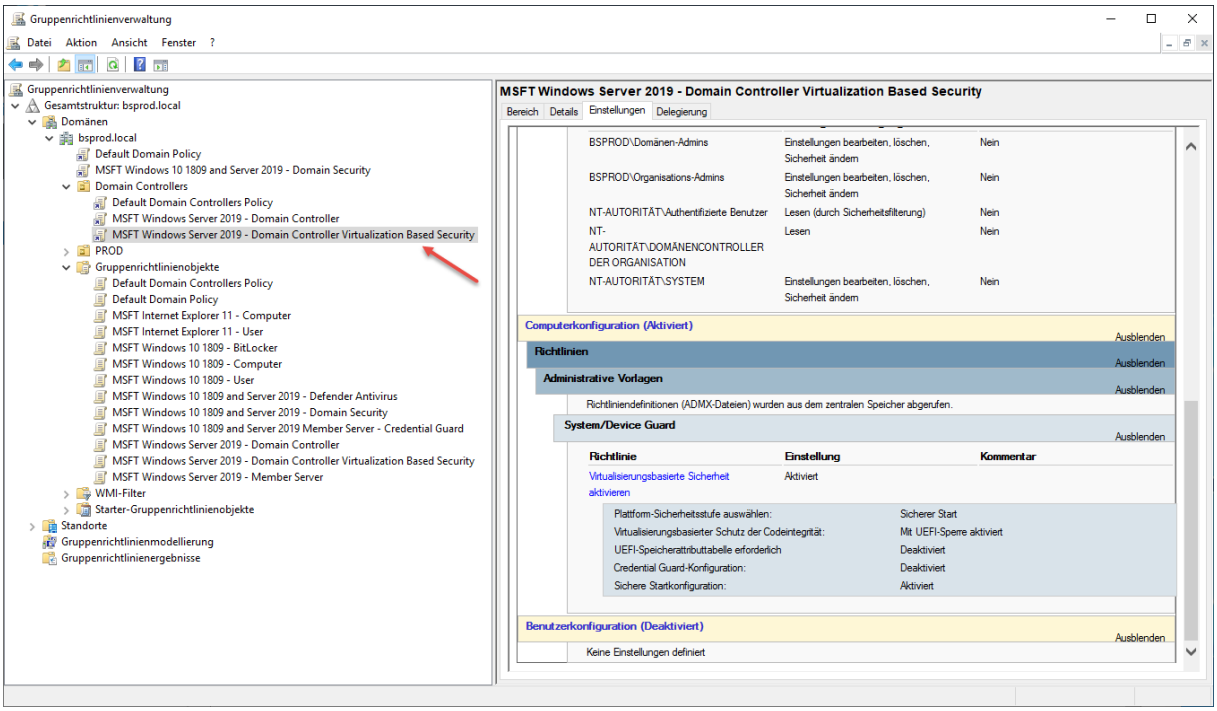


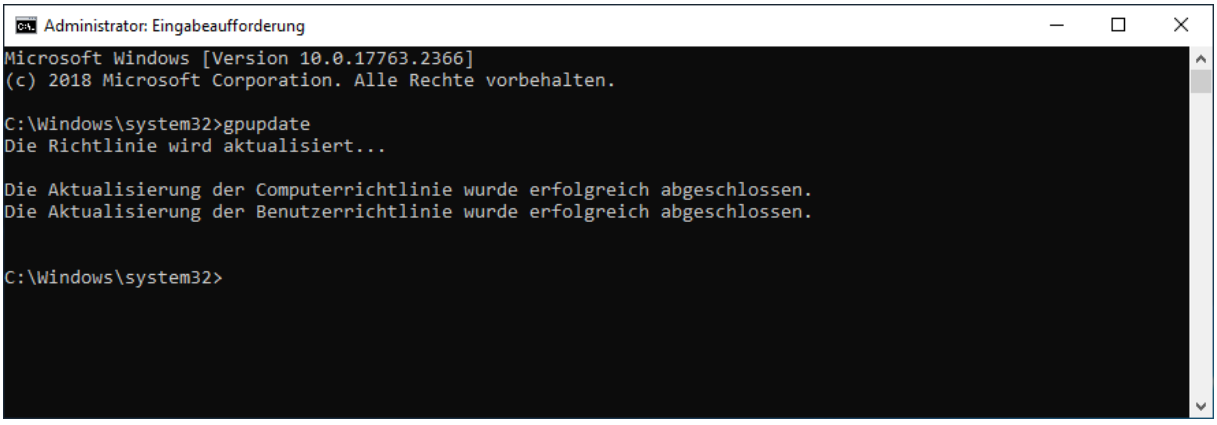
{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Schauen wir uns, die auf die Domain Controller verlinkten GPOs mal etwas genauer an. Jetzt wird klar, dass es sich um die Richtlinie zur Aktivierung von VBS (Virtualization Based Security) / Device Guard handelt.

Es scheint, dass die Abhängigkeiten zuvor gar nicht evaluiert bzw. eingerichtet/konfiguriert wurden und deswegen der Fehler ausgegeben wird. Entweder entfernt man die fälschlicherweise verlinkte Richtlinie oder aktiviert/installiert die Abhängigkeiten damit VBS eingesetzt werden kann.

Ich entferne die Richtlinie, weil meine virtuelle Maschine die benötigten Abhängigkeiten nicht besitzt. Die Virtualisierungs-basierten Sicherheitsfunktionen nutzen eine Reihe von Sicherheitselementen wie UEFI, Secure Boot und Trusted Platform Module (TPM) 2,0.





Virtualisierungsbasierte Sicherheit (VBS)

Grundlegende Schutzmaßnahmen und zusätzliche Qualifikationen für den virtualisierungsbasierten Schutz der Codeintegrität

Windows Defender Credential Guard: Anforderungen

{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Die CSE-GUIDS lassen sich mithilfe der Powershell aus der Registrierung auslesen:

Get-ChildItem "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions" | Out-GridView