

## <u>Inhalt</u>

Ausgangssituation	2
ADMX-Dateien und der Central Store	2
Das Problem: Anzahl möglicher Betriebssysteme im Active Directory	4
Problemszenario 1: entfernte Konfigurationsoption	5
Problemszenario 2: Veränderung einer Einstellung #1	8
Problemszenario 3: Veränderung einer Einstellung #2	9
Problemszenario 4: Clientseitige Veränderungen	12
Problemszenario 5: neue ADMX-Dateien durch Windows Updates	13
Die administrative Lösung bzw. der WorkAround	13
Bereitstellung von GPO für ein neues Betriebssystem	15
Referenzsystem erstellen	15
GPO bereitstellen	21
GPO Sicherheit (SCT-Baseline)	27
GPO Datenschutz	31
GPO Konfiguration	34
Kompatibilität sonstiger GPO	34
Vergleich zwischen zwei GPO mit dem PolicyAnalyzer (SCT)	
GPO anwenden	44
Testlauf	46

## **Hintergrundinformation**

#### **Ausgangssituation**

Windows Administratoren können im Active Directory mit Gruppenrichtlinien zentral Einstellungen und Konfigurationen an eine Vielzahl von Clients und Benutzern automatisiert verteilen. Das Werkzeug ist mächtig und es wird seit Generationen von Betriebssystemen verwendet.

Wenn Microsoft ein neues Betriebssystem auf den Markt bringt, dann enthält dieses eigentlich immer Funktionen, welche die Vorgänger nicht hatten. Damit auch diese über Gruppenrichtlinien gesteuert werden können, gibt es mit jedem neuen Betriebssystem auch neue Versionen der Gruppenrichtlinien-Vorlagen. Diese sind als **ADMX** bekannt: **ADM**inistrative templates ne**X**t generation. Die Vorgänger waren ADM-Dateien. Es besteht eine gewisse Analogie zum Wechsel von \*.doc auf \*.docx.

Jede neue Generation von ADMX-Dateien sollte das aktuelle Betriebssystem und alle Vorgänger steuern können. Wir Administratoren mussten also nur die neusten Vorlagen in den richtigen Speicherplatz kopieren und schon konnten wir in der Management-Konsole für die Gruppenrichtlinien loslegen.

Beim Konfigurieren von Einstellungen mussten wir nur auf dieses Feld achten und alles wurde gut:



Das Prinzip wurde auch als "SuperSet" bezeichnet. Ein schöner Gedanke an die vergangenen Tage!

#### ADMX-Dateien und der Central Store

Wie funktionieren die ADMX-Vorlagen? Dazu habe ich in einem Gruppenrichtlinien-Workshop eine Zeichnung erstellt:



Die Vorlagen liegen immer im Verzeichnis C:\Windows\PolicyDefinitions. Öffnet man einen Editor für eine Gruppenrichtlinie (auch aus der Gruppenrichtlinienverwaltung für das Active Directory), dann werden die Vorlagen geladen und unter Computer|Benutzer\Policies\Administrative Templates eingebunden. In den ADMX sind dann die Anweisungen

enthalten, wie die Formulare im Editor auszusehen haben und welche Werte dann in die GPO geschrieben werden sollen. Das könnte so aussehen:



Ein Client läd nun die für ihn definierten Gruppenrichtlinien aus der SYSVOL-Freigabe als Dateien herunter und wendet sie lokal an.

Die ADMX-Dateien sind für uns lesbar: Sie sind in einem XML-Format strukturiert:



Mit "Superset" musste man immer nur die neusten ADMX-Vorlagen verwenden. Damit das in größeren Infrastrukturen kein Problem wird (es kann hier durchaus mehr als einen Editorrechner geben), kann man diese Dateien in ein spezielles Verzeichnis kopieren: Den Central Store. Dieser Speicherort kann im gleichen Verzeichnis wie die fertigen Gruppenrichtlinien erstellt werden:



📕 🛛 🚽 🖛 🛛 Windows		- 🗆 X	📙   🛃 🚽   Policies			- 🗆 X
File Home Share	View	~ 🕐	File Home Share View			~ 😮
Pin to Quick Copy Paste	Move to * X Delete * Copy to * A Rename New folder	roperties	Pin to Quick Copy access Copy Date	Move Copy to to t	Perties	Select all Select none
Clipboard	Organize New	Open Select	Clipboard	Organize New	Open	Select
← → × ↑ 📜 « SYST	EM (C:) > Windows  v ひ Se	earch Windows 🔎	← → ✓ ↑ 📕 C:\Windows\SYSVOL	\domain\Policies v	Search Policies	م
Program Files (x86)	^ Name ^	Date mod ^	ShellExperiences	^ Name	Date modified	Туре ^
Users	Migration	16.07.201	SKB	{581A4166-09A2-46D2-A40D-60B11DFC	25.11.2019 07:34	File folder
📜 Windows	MiracastView	26.06.201ł	SoftwareDistribution	{7591C504-D294-4EBB-9BFE-FDA911DC	15.10.2018 07:29	File folder
ADFS	ModemLogs	16.07.201( 6.	Speech	{8191DA7C-9700-4FCE-AD51-75509933	15.10.2018 07:29	File folder
ADWS	NTDS	30.01.202(	Speech_OneCore	{39752A12-541F-4552-9DA3-EB388406D	15.10.2018 07:38	File folder
appcompat	OCR	16.07.201	System	{5139387A-8592-4ED5-835C-21B647D5F	15.10.2018 07:29	File folder
AnnPatch	Offline Web Pages	16.07.201	System 32	{08800482-F55B-41A6-96BA-6C37267BA	15.10.2018 07:38	File folder
AppReadiness	Panther	26.06.201	System See	{52256374-B713-46CA-8046-9885617247	10.12.2019 14:24	File folder
Appreadiness	Performance	16.07.201	SystemApps	B8A8D764-F140-4A9D-AE3C-FF5FDED7	25.11.2019 17:05	File folder
assembly	PLA	16.07.201	SystemResources	{B89429BB-9E4B-4F2D-982A-08D2C51B	15.10.2018 07:33	File folder
bcastdvr	PolicyDefinitions	31.01.02	SYSVOL	BA00CBA5-082A-4DA6-A191-08A03E58	15.10.2018 07:29	File folder
Boot	PrintDialog	26.06.201	domain	BDF5AB9C-F5AA-4140-89B2-5C7A0CE2	15.10.2018 07:29	File folder
Branding	Provisioning	16.07.201	Policies	{D12FB4BE-5404-410F-9F1F-42270DF61B	25.11.2019 07:32	File folder
CbsTemp	Registration	16.07.201(	scripts	{DC75FB51-64ED-49E7-86D6-CEC171108	25.11.2019 17:02	File folder
Cursors	RemotePackages	16.07.201	📕 staging	▲ {F7F1D6DD-E174-4A26-BC32-5852DEEE	15.10.2018 07:33	File folder
debug	rescache	15.10.201	staging areas	FCE91AA1-2B9C-40B8-B6E3-192F07630	25.11.2019 07:32	File folder
diagnostics	Resources	16.07.201( 🗸		PolicyDefinitions	16.07.2016 18:21	File folder 🗸
	~ <	>	sysvoi	v <		>
94 items 1 item selected			33 items 1 item selected		Activate	e Window 📰 📰

Ab diesem Moment bezieht sich der Gruppenrichtlinieneditor immer auf den Central Store und verwendet die Vorlagen aus diesem Verzeichnis. Der Pfad wird dabei über die SYSVOL-Freigabe der Domain angesprochen:



Damit war das SuperSet sehr einfach umsetzbar.

#### Das Problem: Anzahl möglicher Betriebssysteme im Active Directory

In allen Windows Server Kursen von Microsoft und in fast allen Internet-Ressourcen gehen wir von diesem Idealfall des "SuperSet" aus. Aber mit jedem weiteren Betriebssystem wurde es wohl für Microsoft komplizierter, diese Abwärtskompatibilität zu gewährleisten. **Die Entwickler konzentrierten sich meist nur noch auf das neue System**.

Naja, so oft kommen doch keine neuen Betriebssysteme raus, oder? Falsch: Jedes Jahr veröffentlicht Microsoft zwei neue Releases durch den Semi Annual Channel! Und damit wird das Problem immer größer. Mittlerweile haben wir unter Berücksichtigung des Extended Security Support folgende mögliche Versionen mit Support (**Stand 31.01.2020**):

Betriebssystem	Support von	Support bis	Support-Hinweis
Windows 7	22.10.2009	14.01.2020 +3a	max. 3 Jahre Extended Security
Windows 8.1	18.10.2013	10.01.2023	
Windows 10 1709	17.10.2017	14.04.2020	nur mit Enterprise Edition
Windows 10 1803	30.04.2018	10.11.2020	
Windows 10 1809	13.11.2018	11.05.2021	nur mit Enterprise Edition
Windows 10 1903	21.05.2019	08.12.2020	
Windows 10 1909	12.11.2019	10.05.2022	nur mit Enterprise Edition
Windows 10 LTSB 2015	29.07.2015	14.10.2025	nur mit Enterprise Edition
Windows 10 LTSB 2016	02.08.2016	13.10.2026	nur mit Enterprise Edition
Windows 10 LTSB 2019	13.11.2018	09.01.2029	nur mit Enterprise Edition
Windows Server 2008R2		14.01.2020 +3a	max. 3 Jahre Extended Security
Windows Server 2012	30.10.2012	10.10.2023	
Windows Server 2012R2	25.11.2013	10.10.2023	

Windows Server 2016	15.10.2016	12.01.2027	
Windows Server 2019	13.11.2018	09.01.2029	

In der Liste habe ich mal die Windows Server mit Semi Annual Channel ausgespart.

Die spannende Frage lautete für mich: "Ab wann war die Abwärtskompatibilität der Gruppenrichtlinien nicht mehr garantiert?". Dazu habe ich einen Artikel bei Microsoft gefunden: Das Problem mit den Vorlagen ohne komplette Abwärtskompatibilität existiert seit Windows Server 2012 und Windows 8:

Microsoft	Office	Windows	Surface	Xbox	Deals	Support	More ~	Search for help
Windows sup	port	Downloads	Community					

## An update is available to enable the use of Local ADMX files for Group Policy Editor

Applies to: Windows 8.1 Enterprise, Windows 8.1, Windows 8.1 Pro, More

Update Available

#### Symptoms

This article describes an update that allows you to configure the Group Policy editor to use Local ADMX files instead of the Central Store.

Assume that you use updated ADMX files in the central store on SYSVOL for Group Policy tools on a domain controller. Group Policy Management Console (GPMC) on clients uses the ADMX files in the central store instead of the local store.

In this situation, some settings cannot be configured for computers that are using the previous versions of the ADMX files. The settings appear i the editor as "extra registry settings." The new ADMX files in the domain central store do not contain the editor meta-data for these settings.

Note Settings that are made prior to the upgrade of the ADMX central store apply to the clients, but cannot be edited anymore.

#### Cause

This issue occurs because the updated ADMX files may not contain some settings for older versions of the operating system.

#### https://support.microsoft.com/en-us/help/2917033/an-update-is-available-to-enable-the-use-of-local-admx-files-forgroup

Damals war ein Hotfix für einen Workaround verfügbar, dessen Funktion mittlerweile als Standard in allen Betriebssystemen enthalten ist. Diesen Workaround erläutere ich weiter unten.

OK, dann gibt es einige Einstellungen nicht mehr. Was soll schon passieren, fragt ihr euch? Da gibt es einige Szenarien...

#### Problemszenario 1: entfernte Konfigurationsoption

Microsoft ersetzt eine ADMX-Datei durch eine neue Version. Wenn ihr die alte Version vorher für eine bestehende GPO verwendet habt, dann kommt ihr mit der neuen Vorlage eventuell nicht mehr an die konfigurierten Einstellungen heran. Man erkennt solche Elemente an den "Extra Registry Settings" im Report der GPO.

Hier sieht man eine GPO, die ich mit den ADMX-Dateien von Windows Server 2008R2 erstellt habe. Die gleichen Einstellungen erreiche ich auch mit den Vorlagen vom Windows Server 2012R2:

Group Policy Management Editor			_		×
File Action View Help					
<table-cell-rows> 🔶 📶 🗟 📓 🐨</table-cell-rows>					
> 🧮 Group Policy	^	Setting	State		
> Internet Communication Managem		Configure the level of TPM owner authorization information	Not configu	ured	
> iscsi		Configure the list of blocked TPM commands	Not configu	ured	
KDC		Ignore the default list of blocked TPM commands	Not configu	ured	
Kerberos		Ignore the local list of blocked TPM commands	Not configu	ured	
Locale Services		Standard User Individual Lockout Threshold	Enabled		
Logon		Standard User Lockout Duration	Not configu	ured	
Power Management		Standard User Total Lockout Threshold	Not configu	ured	
		Turn on TPM backup to Active Directory Domain Services	Enabled		
Remote Assistance					
Remote Procedure Call					
Removable Storage Access					
Scripts					
Server Manager					
Shutdown					
Shutdown Options					
System Restore					
> Troubleshooting and Diagnostics					
Trusted Platform Module Services					
User Profiles					
Windows File Protection					
> Windows Time Service					
> Windows Components					
All Settings					
> Preferences					
🐒 User Configuration					
> Policies			_		
> Preferences	~	Constant Constant (			>
· · · · · · · · · · · · · · · · · · ·		Extended Standard			
8 setting(s)					

**VS IT-Solutions** 

Mit den Vorlagen eines Windows Server 2016 und 2019 kann ich auf eine Einstellungen nicht mehr zugreifen:



Vielleicht wird diese nicht mehr ab Windows Server 2016 benötigt. Aber wenn ich noch "alte" Windows Server 2012R2 im Einsatz habe, wie kann ich die Einstellung nachträglich anpassen?

Die gesetzte Einstellung in der registry.pol-Datei ist dabei natürlich immer noch vorhanden:

# WS IT-Solutions WSHowTo – moderne GPO-Versionierung am Beispiel Windows 10

	inistrator: Windows PowerShell ISE – 🗌	$\times$
File Edit	it View Tools Debug Add-ons Help	
1		
Untitleo	d1.ps1* X	
6 7 8	<pre>Scontent = Get-Content -Path 'C:\Windows\SYSVOL\domain\Policies\{D056293A-BB54-4543-8791-C32D4BBCFFE7}\Machine\Registry.pol' -encoding unicode</pre>	• ^
10	<pre>\$content -replace '\]\[',"]`r`n["</pre>	
<		>
[Sof [Sof	<pre>tware\Policies\Microsoft\TPM ;RectiveDirectoryBackup ; ; ] tware\Policies\Microsoft\TPM ;RequireActiveDirectoryBackup ; ; ]</pre>	
PS C	i: \>	

Das bedeutet, kompatible Clients werden die Einstellung immer noch anwenden. Man kommt nur nicht mehr an die Schalter im Frontend heran. Im Vergleich der beiden ADMX-Dateien sieht man schön den Unterschied. Hier ist die Einstellung bis Windows Server 2012R2 vorhanden:



Die neue Vorlage ab Windows Server 2016 sieht dagegen so aus:



So wird eben nichts mehr angezeigt! Viel Spass beim TroubleShooten!

#### Problemszenario 2: Veränderung einer Einstellung #1

Jedes Editor-Formular wird mit den Definitionen einer ADMX aufgebaut. Setzt man darin eine Einstellung auf z.B. "aktiviert", dann wird im Hintergrund in einer Datei im Sysvol ein Wert in einer Datei eingetragen. Hier seht ihr ein einfaches Beispiel:



Den Wert bestimmt der Inhalt der dazugehörigen ADMX-Datei. Sie gehört einem Windows Server 2016:

<policy name="AllowProjectionToPC" class="Machine" displayName=</pre> "\$(string.AllowProjectionToPC)" explainText= "\$(string.AllowProjectionToPC\_help)" key= "Software\Policies\Microsoft\Windows\Connect" valueName="AllowProjectionToPC"> <parentCategory ref="Connect" /> <supportedOn ref="windows:SUPPORTED Windows 10 0 NOSERVER" /> <enabledValue> <decimal value="0" /> </enabledValue> <disabledValue> <decimal value="1" /> </disabledValue> </policy>

Es kommt selten vor: Microsoft ändert auch die hinterlegten Werte in den ADMX! Die gleiche GPO-Einstellung von eben öffne ich mit einem GPO-Editor, der auf die ADMX-Dateien eines Windows Server 2019 zugreift:



Was ist denn hier passiert?? Ganz einfach: in der neuen ADMX steht der Wert für "aktiviert" mit einem anderen Wert:

<pre><policy class="Machine" displayname="&lt;/pre" name="AllowProjectionToPC"></policy></pre>
"\$ (string.AllowProjectionToPC) " explainText=
"\$(string.AllowProjectionToPC help)" key=
"Software\Policies\Microsoft\Windows\Connect" valueName="AllowProjectionToPC">
<pre><parentcategory ref="Connect"></parentcategory></pre>
<pre><supportedon ref="windows:SUPPORTED Windows 10 0 NOSERVER"></supportedon></pre>
<pre><denabledvalue></denabledvalue></pre>
<pre><decimal value="1"></decimal></pre>
<disabledvalue></disabledvalue>
<decimal value="0"></decimal>

Öffnet man nun den Editor mit der neuen ADMX-Datei, dann ließt er die bereits konfigurierte Einstellung und zeigt in der grafischen Oberfläche den korrespondierenden Wert lauf der XML-Information an. Aus einem "aktiviert" wird ein "deaktiviert".

Ein Betriebssystem, dass mit genau dieser ADMX ausgeliefert wurde, wird die Einstellung lokal bestimmt richtig interpretieren. Was ist aber mit den anderen Betriebssystemen? Und was passiert, wenn ihr diese Einstellung auf einem Windows Server 2016 auf "aktiviert" (also mit dem Wert 0( konfiguriert und durch ein Update auf einmal eure Clients mit Windows 10 1809+ laufen? Die Clients sehen in der registry.pol-Datei im SYSVOL nur eine 0 – und interpretieren sie als "deaktiviert"... Viel Spass beim TroubleShooting!

#### Problemszenario 3: Veränderung einer Einstellung #2

Diese Einstellung habe ich unter "Computer\Policies\Administrative Templates\Windows Components\Windows Update" gefunden. Die ADMX-Dateien stammen von einem Windows Server 2008R2. Damals stand die Gültigkeit ab Windows Vista beschrieben:



Im Hintergrund wird die Einstellung in einer registry.pol-Datei abgelegt. Diese kann ich mit der PowerShell anzeigen:





Wenn ich nun die ADMX-Dateien auf Windows Server 2012R2 aktualisiere und die gleiche GPO öffne, dann wird mir folgendes Bild im Editor angezeigt:

Smart Card	Setting	State	Comment	Previous Setting	Next Setting	]
Store Sync your settings Tablet PC Tablet PC Tablet PC Tablet PC Tablet PC Mindows Color Syste Windows Color Syste Windows Tweiler Windows Meror Report Windows Meror Report Windows Media Drigt Windows Media Digt Windows Media She Windows Mesenger Windows Remote Ma Windows Remote She Windows Update Setting(s)	Le nois capey missi upoates and shut Down option in shut Down     Do not adjust default option in Shut Down     Tabling Windows Update Power Management to automatu,     Always automatically retart at alt the scheduled time     Specify intranet Microsoft update service location     Automatic Updates at the scheduled time     Specify intranet Microsoft update service location     Automatic Updates     Specify intranet Microsoft update service location     Automatic Updates     More automatic Updates     Torn on connect to any Windows Update Internet locations     Turn on Software Notifications     Molw Automatic Updates immediate installation     Turn on recommended updates via Automatic Updates     No auto-restart with logged on users tocheduled automatu.     Reprompt for estant with objeged on users tochedule installations     Bable Retart for scheduled installations     Enable client-side targeting     Allow signed updates scheduled installations     Enable client-side targeting     Allow signed updates from an intranet Microsoft update ser.  <<	Not configured Enabled Not configured Not configured	No No No No No No No No No No	Vectorfigured  Vector	Supported on:	Windows Server 2006, Windows 7, and Windows Yota           Help:

Die Einstellung ist natürlich weiter aktiv, da die zugehörige registry.pol-Datei im SYSVOL zwischenzeitlich nicht verändert wurde. Aber offensichtlich gilt die Regel nicht länger für die derzeit modernen Betriebssysteme Windows 8 und Windows 8.1.

Wie schaut es aus, wenn ich die ADMX-Dateien auf Windows Server 2016 aktualisiere?

File Action View Help + + 2 TO - B I TO T > Tablet PC ^ Setting			and French Press and a		
				on Handaka Dauran S.	demonstrate and an extension of the content of the second se
> Tablet PC  Setting			Enabling windo	vs opdate Power n	vanagement to automatically wake up the system to install scheduled updates
Task Scheduler     Windows Calendar     Windows Calendar     Windows Calendar     Windows Calendar     Windows Cuttomer Ex     Windows Defender     Windows Defender     Windows Defender     Windows Nerre Report     Windows Hour Rore     Windows Netail     Specify active hours range for auto-test     Windows Netail     Specify active hours range for auto-test     Windows Netail     Specify active hours range for auto-test     Windows Netail     Windows Netail     Specify active hours range for auto-test     Windows Netail     No auto-restat noteret     Windows Netail     No auto-restat with Nogedo un usenf	State Down' option in Sh.	Comme A No No No No No No No No No No No No No	C Options:	Next Setting Comment: Supported on:	Windows Server 2008, Windows 7, and Windows Vista <ul></ul>

Das sieht nach dem Idealfall aus. So war das Prinzip "SuperSet" gedacht. Die noch neuere Version hält die Legacy-Einstellung weiter vor und deren Wirkungsbereich wurde nicht verändert.

So wird es mit den ADMX-Dateien unter Windows Server 2019 weitergehen, oder?

I Group Policy Management Edi	tor			Teachline Minder	n Mardata Davisa N	Verseen the set of the
File Action View Help				Enabling window	is update Power in	wanagement to automatically wake up the system to install sc
🗢 🔿 📶 🔂 🖬 🖬	T			Enabling Window	vs Update Power I	Management to automatically wake up the system to install scheduled updates
Windows Custome Experie A Windows Defender Antivin Windows Defender Exploit Windows Defender Exploit Windows Telender Exploit Windows Heilo for Busines Windows Intaller Windows Intaller Windows Mesia Digatal Rig Windows Mesia Digatal Windows Remote Manager Windows Remote Shell Windows Security Windows Security	Setting Windows Update for Business Do not diguted for Business Do not adjust default option to "Install Updates and Shut Down" option in Sh Do not adjust default option to "Install Updates and Shut Down" option in Sh Do not adjust default option to "Install Updates and Shut Down" option in Sh Di Do not adjust bours ange for auto-restarts Databating Wundows Update Bours Research and the scheduled time Di Specify deates be downloaded automnticially over metere Databating Wundows Update Bours State Shut Down Di Specify deates be downloaded automnticially over metere Di Specify deate be downloaded automnticially over metere Di Specify deate-restart reminden notifications for update installations Configure Auto-restart reminden softwares Do not allow optate defaults optices to cause cans against Do not allow update defaults over Updates 'Enture B. Benove access to use all Windows Update Internet locations Data Ministraton To receive update notifications Data Specify Engaged restart transition and notification schedule Do not allow the Windows Update Specify Updates Specify Engaged restart transition and notification schedule Do Dont allow 3.Standard /	State Not configured Not configured	Comme A No No No No No No No No No No No No No	Previous Setting	Next Setting Comment: Supported on:	Windows Server 2008, Windows 7, Windows Vista, and Windows 10         Image: Control of the server of the serv

Nanu? Die Einstellung ist auf einmal nicht mehr konfiguriert?? Und plötzlich kann auch Windows 10 wieder damit umgehen? Aber Windows 10 gab es doch schon mit Windows Server 2016? Sind vielleicht nicht alle Versionen gemeint? Was ist da los?

Zur Info: Die Einstellung ist im Hintergrund immer noch vorhanden und alle AMDX-Versionen der Windows Updates bis Windows Server 2016 erkennen die Einstellung auch:



Das bedeutet, die neue Windows Server 2019 ADMX erkennt beim Laden der GPO den Registry-Pfad in der Registry.pol nicht. Aber was passiert dann, wenn ich den Schalter wieder aktiviere?

Group Policy Management Edito	if .		– 🗆 X'	Enabling Window	ws Update Power N	fanagement to automatically wake up the system to install sc $ \Box$ $ imes$
File Action View Help	Ŧ			Enabling Windo	ws Update Power I	Management to automatically wake up the system to install scheduled updates
Windows Customer Experie Windows Defender Antwin Windows Defender Exploit Windows Defender SmartS- Windows Error Reporting Windows Hello for Busines Windows Inkt Workspace Windows Inktaller	Setting Windows Update for Business Do not display 'Install Updates and Shut Down' option in Sh Do not adjust default option to 'Install Updates and Shut Do Trabiling Windows Update Power Nanagement to automatu. Turn of auto-restart for updates during active hours Dependent to be dependended automatically care meters	State Not configured Enabled Not configured Not configured Not configured	Comm A No No No No No	Not Configured     Enabled     Disabled	Comment: Supported on:	Windows Server 2008, Windows 7, Windows Vista, and Windows 10
<ul> <li>Windows Logon Options</li> <li>Windows Media Digital Rig</li> <li>Windows Media Player</li> </ul>	Anow opauter to be dominated automatedly of the needed.     Anow opauter to be dominated automatedly of the needed.     Specify deadline before auto-restart for update installation	Not configured Not configured	No No	Options:		Help:
Windows Messenger Windows Nobility Center Windows PowerShell Windows Reliability Analys Windows Remote Manager Windows Remote Shell Windows Security Windows Update Windows Update Windows Update	Configure auto-restart reminder notifications for updates     Turn off auto-restart notifications for updates     Configure auto-restart required notification for updates     Configure Automatic Updates     Configure     Configure Automatic Updates     Configure     Co	Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	No No No No No No No	5		Specifies whether the Windnows Update will use the Windnows Power Management features to automatically wake up the system from sleep, if there are updates scheduled for installation. Windnows Update will only automatically wake up the system if Windnows Update is configured to install updates automatically. If the system is in sleep when the scheduled install time occurs and there are updates to be applied, then Windnows Update will use the Windows Power management features to automatically wake the system up to install the updates.

Das hat funktioniert. Und was steht nun in der Registry.pol-Datei?

📔 🔽 🔻   Machine			- 0	×
File Home Share View			2	^ 🕐
to Quick Copy Paste Clipboard	Acve Copy Delete Rename Dide Copy Organize New New	n • ess • Deen • Properties Open	Select all Select none Invert selection Select	
→ 👻 🛧 📕 « Policies > (BCCFD80	C5-359C-47CE-A300-9FAA580D2627} > Machine	v Ü S	earch Machine	ρ
415CAF84-241A-4053-E ^	Name	Date modified Type	Size	
[/31A6B00-D219-48BC-	comment.cmtx	04.02.2020 08:37 CMT	X File 1 KB	
[9460EECS-3601-484F-8 [15433BE4-8A19-4FB7-E]	Registry.pol	04.02.2020 08:37 POL	File 1 KB	
(23512502-0D08-4580-E	Administrator: Windows PowerShell ISE			
[B51A7982-BE23-4DB0-	File Edit View Tools Debug Add-ons	Help		
BA520AA9-BEB7-451C-	1 😂 🖬 🔏 🖨 🔪 🖆	. 🖓 🕨 🖬 🖬	* 8 8 0	
BCCFD8C5-359C-47CE-			the second se	
Machine	BE CULL Cat Contant Bath (Cull	tindows) system \ down		E 250c 47cr A200 0rAA580026271\Machine\Desistry pol' encoding up
User (DEC3DBAE-1B7B-4D97)	PS C: (> Get-Content -Path C: ( 剤来 [Software\Policies\Microso rManagement ; ; ; ]	ft\windows\windowst	Jpdate ; AUPowerManager	<pre>which is a set of the set of</pre>
E80D2E65-87B6-4707-4	PS C:\>			

Seht ihr den fast identischen, doppelten Eintrag in der registry.pol-Datei? Das darf nicht wahr sein: Microsoft hat in der ADMX-Datei einfach den Pfad des Registry-Keys geändert. Daher wurde die alte Einstellung auch nicht mehr erkannt! Hier sieht man die Konfiguration der ADMX-Datei von Windows Server 2016:

Und hier die gleiche Einstellung in der ADMX-Datei eines Windows Server 2019:



Nur wissen denn das jetzt auch die alten Betriebssysteme? Die müssen ja zur richtigen Zeit an der richtigen Stelle in der Registry nach der Konfiguration suchen. Wenn die dazugehörige GPO aber den falschen Pfad abspeichert, weil die entsprechende ADMX-Datei nicht für das Zielbetriebssystem gebaut wurde, dann wird das nichts! Viel Spass beim TroubleShooting!

#### Problemszenario 4: Clientseitige Veränderungen

Ebenso kann die Interpretation von Einstellungen im Client problematisch werden. Ich habe einen Bekannten, der seine Clients über einen WSUS aktualisiert. Die Konfiguration dazu lief immer problemlos über eine GPO: Die Clients besuchten den WSUS-Server und installierten brav die dort genehmigten Updates. Die Featureupdates wurden aber für interne Tests zurückgehalten. Ein Standard in Firmenumgebungen.

Eines Tages installierten alle Clients fast gleichzeitig ihre Betriebsversion auf das neuste Release von Windows 10! Dabei war dieses Update nicht freigegeben! Was war passiert? Die Clients wurden durch ein vorheriges Featureupdate bewusst aktualisiert. Die neue Version war aber nicht mit der alten GPO kompatibel und die Systeme ignorierten die Einstellung für Windows Updates komplett. Danach arbeiteten sie im Standardmodus und gingen einfach zum Windows Update Service

im Internet. Mit dessen Updates hielten sie sich aktuell. Bis das nächste Featureupdate anstand – das intern nicht genehmigt war. Und die nicht genehmigte Installation startete.

Und meine eigene Infrastruktur hatte das Problem auch schon, dass eine funktionierende GPO auf einmal nicht mehr wirkte: <u>https://www.ws-its.de/wshowto-wsus-und-clients-melden-100-aber-einige-updates-fehlen/</u>

#### Problemszenario 5: neue ADMX-Dateien durch Windows Updates

Administratoren legen gerne die passenden ADMX-Dateien im Central Store im Active Directory SYSVOL-Share ab. Die Dateien bekommt man aus dem Verzeichnis C:\Windows\PolicyDefinitions des Zielbetriebssystems.

Nach dem Prinzip "SuperSet" sollten hier die ADMX-Dateien des neusten Betriebssystems abgelebt werden. Man installiert also ein Referenz-System und hat Zugriff auf die Dateien. Bis zum nächsten FeatureUpdate oder bis zur nächsten Version des Betriebssystems gibt es keine Veränderungen mehr.

Leider stimmt auch diese Annahme nicht (mehr): Microsoft passt auch bereits veröffentlichte Betriebssysteme an. Hier sieht man schön die unterschiedlichen Datumswerte auf einem Windows Server 2016:

📙 🛛 🚽 📕 🔻 🛛 PolicyDefinitions			_		$\times$
File Home Share View				/	~ ?
Pin to Quick Copy access Copy Paste	Move Copy to to t	item • access • Properties	t Select all	on	
Clipboard	Organize New	Open	Select		
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\blacksquare$ C:\Windows\PolicyD	efinitions	v ري	Search PolicyDefin	nitions	ρ
MiracastView	Name	Date modified	Туре	Size	^
ModemLogs	WindowsProducts.admx	16.07.2016 15:19	ADMX File	10 KB	
NetworkController	WindowsRemoteManagement.admx	16.07.2016 15:19	ADMX File	11 KB	
NTDS	WindowsRemoteShell.admx	16.07.2016 15:19	ADMX File	5 KB	
OCR	WindowsServer.admx	16.07.2016 15:19	ADMX File	2 KB	
Offline Web Pages	WindowsStore.admx	16.07.2016 15:18	ADMX File	6 KB	
Panther	WindowsUpdate.admx	28.03.2017 04:52	ADMX File	40 KB	
	Winlnit.admx	16.07.2016 15:19	ADMX File	3 KB	
Performance	WinLogon.admx	16.07.2016 15:19	ADMX File	6 KB	
PLA	WinMaps.admx	16.07.2016 15:18	ADMX File	3 KB	
PolicyDefinitions	Winsrv.admx	16.07.2016 15:19	ADMX File	2 KB	
📕 PrintDialog	WirelessDisplay.admx	16.07.2016 15:19	ADMX File	2 KB	
Provisioning	wlansvc.admx	16.07.2016 15:19	ADMX File	4 KB	
Registration	WordWheel.admx	16.07.2016 15:19	ADMX File	2 KB	
RemotePackages	WorkFolders-Client.admx	16.07.2016 15:19	ADMX File	3 KB	
rescache	WorkplaceJoin.admx	16.07.2016 15:18	ADMX File	2 KB	
Resources	WPN.admx	16.07.2016 15:19	ADMX File	6 KB	
	wwansvc.admx	16.07.2016 15:19	ADMX File	3 KB	~
197 items 1 item selected 39,2 KB					-

Dies geschieht üblicherweise durch die monatlichen Updates. Da sind eben nicht nur Sicherheitspatches enthalten. Wird eine lokale Komponente des Betriebssystems angepasst, dann ziehen die lokalen ADMX-Dateien mit. Aber wer denkt schon jeden Monat daran, diese auch in den Central Store zu kopieren?

Die Folge kann man sich wieder gut vorstellen: Man erstellt mit den zentralen, veralteten Vorlagen die Richtlinien für aktualisierte Systeme. Und irgendwie funktioniert da etwas wieder nicht... Viel Spass beim TroubleShooting!

#### Die administrative Lösung bzw. der WorkAround

Die eingefahrene Vorgehensweise der Ablage aller ADMX-Vorlagen im Central Store stellt uns vor ein Problem: In diesem Verzeichnis kann ein Dateiname nur einmal verwendet werden. Und Microsoft versioniert die Vorlagen im Inhalt der ADMX-Dateien und leider nicht im Dateinamen. So kann also immer nur eine Betriebssystemversion zu einer Zeit für die Gruppenrichtlinien-Editierung verwendet werden!

Ich habe immer wieder Firmen gesehen, die unter dem Central Store "Versionsordner" vorhalten. Bevor eine GPO editiert wird, ersetzt man einfach die Vorlagen durch den Inhalt des Versionsordners. Das ist keine praktikable Lösung:

• Zum einen kann man so immer nur ein Betriebssystem zu einer Zeit editieren.

- Dazu werden Veränderungen im SYSVOL immer auf alle Domain Controller repliziert. Da gibt es dann auch Replikationsverzögerungen. Denkt man da immer dran?
- In den GPO-Editoren sehe ich nicht, welche Vorlagenversion gerade geladen ist. Administration ist da eher Glückssache.

Microsoft hat das Problem selber erkannt und im gleichen Dokument wie oben gezeigt einen Workaround vorgeschlagen:

An update is available to enabl 🗙 🕂	
🛛 🔒 https://support.microsoft.com/en-gb/help/2917033/an-update-is-available-to-enable-the-use-of-local-admx-files-for-group	⊠ ☆

#### Resolution

We recommend that you keep the central store with the Windows 7 or Windows Server 2008 R2 ADMX templates. To edit new policies for Windows 8 computers, we recommend that you use a separate Windows Server 2012 computer that has this hotfix installed.

Install update 2919355 in Windows 8.1 or Windows Server 2012 R2. Install the hotfix that is described in this article in Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008 R2.

## Ab Windows 8 und Windows Server 2012 sollen also die Gruppenrichtlinien von einem passenden Betriebssystem editiert werden!

Aber mit dem Central Store ist es doch egal, auf welchem Rechner ich die GPO bearbeite, da die Editoren immer die zentral bereitgestellten Vorlagen verwenden... Hier kommt der Hotfix zum Einsatz. Dieser erweitert die Steuerung, aus welcher Quelle der Editor die ADMX-Dateien bezieht. **Mit dem Hotfix kann ein Registry-Key erstellt werden, der den Client immer seine eigenen Vorlagen verwenden lässt!** 

Der Hotfix war für die Übergangszeit erhältlich. Mittlerweile ist er ein Bestandteil der Betriebssysteme. Daher wurde diese Seite nicht mehr aktualisiert. Die Empfehlung, Clientrichtlinien von einem Windows Server aus zu editieren, lässt sich daher nicht auf Windows 10 übertragen. Für dessen GPO ist ein Windows Server 2016 oder 2019 nur bedingt geeignet, da seit Windows 10 öfter neue Versionen erscheinen als auf der Serverseite (sehen wir mal von den SAC der Serverbetriebssysteme ab, die keine grafische Oberfläche haben und daher nicht für die Editierung von Gruppenrichtlinien geeignet sind). Die Server haben daher nicht die passenden ADMX-Dateien dabei!

#### Daher gelten seit Windows 10 und Windows Server 2016 folgende Regeln für die Bearbeitung von Gruppenrichtlinien:

• Für jedes Betriebssystem muss ein eigener Editor-Rechner mit dem Remote Server Administration Tool (RSAT) für die Gruppenrichtlinienverwaltung und dem RegistryKey bereitgestellt werden. Nur von diesem System dürfen die GPO dieser Betriebssystemversion editiert werden.

- Für jede Version der Clients und Server werden separate GPO benötigt! Nur dann passt die Bearbeitung mit den richtigen ADMX-Dateien und die Verarbeitung der fertigen Richtlinien auf dem dazu kompatiblen Zielsystem zusammen!
- Für Windows 10 bietet sich der Einsatz von WMI-Filtern an, da durch die Feature-Updates entsprechende Versionswechsel zur Normalität werden.

Falls euch mit den weiter oben genannten Problemen eine andere Lösung einfällt: Ich bin neugierig!

Mit diesem Wissen kann man eigentlich auch auf den Einsatz des Central Stores verzichten. Das erspart das Setzen der Registry-Keys auf den Editor-Systemen.

Insgesamt wird unsere GPO-Landschaft bald so aussehen müssen:



Der Aufwand scheint enorm: jedes Jahr müssen GPO auf's Neue erstellt werden! Das klingt dramatisch, ist es aber nicht. Ich habe mir ein System erarbeitet, mit dem die Erweiterung auf ein neues System schnell, unkompliziert und vor allem einfach beim TroubleShooting ist. Denn meine GPO passen einfach immer auf das Zielsystem!

## Bereitstellung von GPO für ein neues Betriebssystem

#### Referenzsystem erstellen

Zuerst benötige ich ein Referenzsystem mit dem gewünschten Betriebssystem. Dieses bringt die erforderlichen ADMX-Dateien mit. In diesem Beispiel möchte ich Windows 10 in der Version 1909 in meiner Infrastruktur bereitstellen. Aktuell habe ich Gruppenrichtlinien bis zur Version 1903 im Einsatz.

Das neue System wird mein GPO-Editorsystem. Ich benötige also hardwareunabhängigen Zugriff. Daher installiere ich den neuen Client in einer virtuellen Maschine auf einem meiner Hyper-V-Hosts. Diese VM erstelle ich mit dem Assistenten:





Danach starte ich die VM und installiere das System:

🖆 Windows Setup		
	Windows <sup>*</sup>	
Installationssprache:	Deutsch (Deutschland)	
<u>U</u> hrzeit und Währungsformat:	Deutsch (Deutschland)	
Tastatur oder <u>E</u> ingabernethode: Geben Sie Ihre Sprache und andere	Deutsch	
© 2019 Microsoft Corporation. Alle Rechte vor	Tortzüsetzen. Behalten.	er
e ever menoren corporatori, nie neurie von		

Der Prozess ist seit Jahren nahezu unverändert. Kurze Zeit später bin ich auf dem Client angemeldet:





Damit ich von diesem Rechner die Richtlinien meiner Domain editieren kann, benötige ich die Remote Server Administrative Tools (RSAT) für die Gruppenrichtlinienverwaltung. Diese werden bei Servern über den Server Manager installiert. Bei Clients sind sie seit einigen Versionen in den Optionalen Features zu suchen:

← Einstellungen			_	×
Optionale Features				
Siehe Verlauf optionaler Features				
+ Feature hinzufügen				
Deutsch optische Zeichenerkennung	435 KB			
A <sup>2</sup> Eingabe Deutsch	86,7 MB			
German handwriting	23,2 MB			

**VS IT-Solutions** 

÷	Einstellungen	
ሴ	Feature hinzufügen	
¢	RSAT: Tools für Active Directory-Zertifikatdienste	1,49 MB
¢	RSAT: Tools für Dateidienste	5,07 MB
¢	RSAT: Tools für die Remotezugriffsverwaltung	6,70 MB
¢	RSAT: Tools für Netzwerklastenausgleich	267 KB
<b>(</b> 3	RSAT: Tools zur Gruppenrichtlinienverwaltung Zu den Tools zur Gruppenrichtlinienverwaltung gehör Gruppenrichtlinien-Verwaltungskonsole, der Gruppenrichtlinienverwaltungs-Editor und der Gruppenrichtlinien-Starter-GPO-Editor.	4,06 MB en die allieren
~	RSAT: Verwaltungshilfsprogramme für die BitLocker-	41,1 KB

Die Installation benötigt administrative Rechte und eine Internetverbindung. Sie dauert nur wenige Sekunden:

← Einstellungen								×
Optionale Features								
Siehe Verlauf optionaler Features								
+ Feature hinzufügen								
A <sup>2</sup> Deutsch optische Zeichenerkennung	435 KB							
A <sup>字</sup> Eingabe Deutsch	86,7 MB							
A <sup>∰</sup> German handwriting	23,2 MB							
Internet Explorer 11	3,20 MB							
Mathematik-Erkennung	33,2 MB							
<b>स्ट्र</b> Microsoft-Remotehilfe	2,89 MB							
OpenSSH-Client	10,1 MB							
RSAT: Tools zur Gruppenrichtlinienverwaltung	35,4 MB							

Für die Richtlinien-Bearbeitung ist ein Domain Join erforderlich. Ich nehme den Client in meine Domain auf und benenne ihn dabei um. Das AD-Computerobjekt platziere ich in der richtigen Organisationseinheit:



	Systemeigenschaften	×		
	Computername Hardware Erweitert	Computerschutz Remote		- 🗆 ×
ge	Folgende Informationen wer im Netzwerk verwendet.	den zum Identifizieren des Computers > System	und Sicherheit > System 🗸 Ö	$\wp$ Systemsteuerung durchsuchen
	Computerbeschreibung: Zum "Heik	Beispiel: "Spielcomputer" oder asisinforr	nationen über den Computer anzeigen	
	Voltsändiger Computername: DESKUDEV Abetsgruppe: WORKGRO		năne X	Mindows10
	Klicken Sie auf "Netzwerk-ID", um ein oder einer Arbeitsgruppe mithilfe eines beizutreten.	Sie konnen den Namen und die Mitgliedschaft ( ändem. Änderungen wirken sich möglicherweis- auf Netzwerkressourcen aus.	es Computers ion. Alle Rechte vorbehalten. e auf den Zugriff	
	Klicken Sie auf "Ändem", um diesen C umzubenennen oder dessen Domäne Arbeitsgruppe zu ändem.	oder Computername: WS-CL6	AMD Ryzen 7 3700X 8-Core Processor 3.60 GHz 2,00 GB	
		Vollständiger Computername: WS-CL6	64-Bit-Betriebssystem, x64-basierter Prozessor Für diese Anzeige ist keine Stift- oder Toucheingabe verfügbar.	
		Mtglied von Domäne:	men, Domäne und Arbeitsgruppe DESKTOP-CIH9F3E	
		OK ws.its O Arbeitsgruppe: WADEKGEDLIP	DESKTOP-CIH9F3E	ändern
		ОК	Abbrechen WORKGROUP	
		Sicke such Windows	st nicht aktiviert. Microsoft-Softwarelizenzbedingungen lesen	
		Sicherheit und Wartung Produkt-II	): 00329-00000-00003-AA173	👽 Windows aktivieren

Durch mein Tier-Management und mein Privileged Access Management haben meine Admin-Accounts keine Rechte. Ich muss die erforderlichen Berechtigungen durch eine temporäre Gruppenmitgliedschaft zuweisen. Mein Account bekommt die Rechte zur Bearbeitung aller GPO (Das Recht habe ich an die Gruppe GG-Admin-GPO delegiert). Zusätzlich bekommt der Administrationsrechte auf der OU, in welcher der neue Client platziert wird. Darin sind auch die Logon-Rechte enthalten (diese würden ausreichen). Die Gruppenmitgliedschaften editiere ich mit meinem PowerShell-GUI-Script "PAM-Admin":

드 PAM-AdminGUI - verbu	unden mit WS-DC1 (Versio	on V1.07)					-		×
Modus: Zeitraum [min]:	Admins 15	Gruppen ~		nac	h DC:	WS-DC2	~	replizie zeige C	eren CMD
Admins:	mõ	igliche Gruppen:		Mitglied:					
admin admin-ata admin-audit admin-backup admin-Notfall admin-setup stephan-T1 stephan-T2 sysadm	Di Di Di Ci Ci Ci Ci Ci Ci Ci Ci Ci Ci Ci Ci Ci	HCP-Administratoren IsAdmins Sadmin-ADJoin S-Admin-ADJoin S-Admin-Reigaben S-Admin-Freigaben S-Admin-Freigaben S-Admin-Setup-Apple S-Admin-Setup-Apple S-Admin-SQL-DPM S-EC-Clients-Standi S-EC-Clients-Standi S-EC-Server-Hyped S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-MB-Ad S-EC-Server-Standi ganisations-Admins Sanisations-Admins	rage ockerAusnahme-AdminDir nins ard-Admins v-Admins ning-Admins mins admins ard-Admins ent	GG-Admin-GPO (n GG-Admin-Setup-) GG-SEC Clents W Protected Users (in	och bis Applocke /SITS-Ao ndirect)	14:39:35) rÅusnahme-ueberall (noch bis 14 dmins (noch bis 14:39:43)	:39:40)		
		hinzufügen		entfernen	er	ntferne alle			
have?									
bereit									

Mit diesen Rechten melde ich mich als Admin am Client an. Weiter geht es in der Gruppenrichtlinien-Verwaltungskonsole:



	9	📓 Gruppenrichtlinienverwaltung									- 🗆 🗙	
Micros	oft Edge	📓 Datei Aktion Ansicht Fe	enster ?								_ 8 ×	
		🗢 🔿 🖄 📅 🗟 🗮 🗙	Q 7									
		🔣 Gruppenrichtlinienverwaltung			^ GPO-Clie	nts-Win10-1903	3-Sicherheit					
_		windows-sichemeit	Produktivität			Einstellungen	Delegierung Status	3				
		Windows-System 🗸 🗸	Troduktivkat			n obsis apzeigen:						
	- <b>I</b> I- •	Windows-Verwaltungsprogramme ^				andorte Domâne	ws.ts en und Omanisationseir	nheiten sind r	nit dem Obiekt verknünft:		¥	
		Aufrahennlanung		e		andore, Deman	F	rzwungen	Verknüpfung aktiviert	Pfad		
		hargabenplanang	Office	Microsoft Edge	Microsoft Store		N	Vein	Ja	ws.its/WS/Clients		
		Computerverwaltung										
		Datenträgerbereinigung										
	Q,	Dienste										
	1	Druckverwaltung									>	
						erung	-		-level			
	0	Ereighisanzeige				er und Computer	nontinienobjekts geiter 7	n nur tur die t	oigenden			
	5	Gruppenrichtlinienverwaltung										
	ŝ,	iSCSI-Initiator				rte Benutzer						
	6	Komponentendienste										
8	B)	laufwerke defragmentieren und g										
_	9											
U	<u>()</u>	Leistungsüberwachung				Er	ntfernen Bş	genschaften				
	14	Lokale Sicherheitsrichtlinie										
ىت	-	ODBC Data Sources (32-bit)				richtlinienobjekt i 103	st mit folgendem WMI-I	Filter verknüp ~	Őffnen			
٢	-	ODBC-Datenquellen (64-Bit)										
¢	ŵ	Registrierungs-Editor										
-	,₽ \$u	chbegriff hier eingeben	C									

Die lokalen ADMX-Vorlagendateien des Clients wurden (wenn überhaupt) für Windows 10 Version 1909 getestet:

📕 🛛 🛃 🗸 🖓 PolicyDe	efinitions					- 0	×
Datei Start Freige	eben Ansicht						~ 🕐
← → ~ ↑ <mark>↓</mark> → □	)ieser PC → Lokaler Datenträger (C:) → Win	dows > PolicyDefinitions		· < 5 v	PolicyDefinitions" durchsuchen		
Help ^	Name	Änderungsdatum	Тур	Größe			^
IdentityCRL	de-DE	05.12.2019 02:19	Dateiordner				
IME	en-US	19.03.2019 13:16	Dateiordner				
ImmersiveC	ActiveXInstallService.admx	19.03.2019 13:19	ADMX-Datei	5 KB			
INF	AddRemovePrograms.admx	19.03.2019 13:19	ADMX-Datei	5 KB			
InputMetho	AllowBuildPreview.admx	19.03.2019 05:46	ADMX-Datei	2 KB			
L2Schemas	AppCompat.admx	19.03.2019 13:19	ADMX-Datei	6 KB			
LiveKernelR	AppHVSI.admx	19.03.2019 13:19	ADMX-Datei	12 KB			
Livekement	AppPrivacy.admx	19.03.2019 05:44	ADMX-Datei	30 KB			
Logs	appv.admx	19.03.2019 13:19	ADMX-Datei	35 KB			
Media	AppxPackageManager.admx	19.03.2019 13:19	ADMX-Datei	5 KB			
Microsoft.N	AppXRuntime.admx	19.03.2019 05:46	ADMX-Datei	4 KB			
Migration	AttachmentManager.admx	19.03.2019 13:19	ADMX-Datei	6 KB			
minidump	AuditSettings.admx	19.03.2019 05:46	ADMX-Datei	2 KB			
ModemLog	AutoPlay.admx	19.03.2019 05:46	ADMX-Datei	4 KB			
OCR	AVSValidationGP.admx	19.03.2019 05:44	ADMX-Datei	3 KB			
	Biometrics.admx	19.03.2019 05:46	ADMX-Datei	4 KB			
Contraction of the second	Bits.admx	19.03.2019 13:19	ADMX-Datei	56 KB			
Panther	Camera.admx	19.03.2019 05:46	ADMX-Datei	3 KB			

Je mehr sich diese Dateien im Vergleich zum Vorgänger verändert haben, je mehr Arbeit ist zu erwarten. Das Änderungsdatum finde ich interessant. Es entspricht dem des Windows 10 Version 1903. Gibt es überhaupt Veränderungen?

	📙 🛛 🗍 PolicyDefir	nitions				- 0	×
Datei	Start Freigebe	en Ansicht					~ 🕐
$\leftarrow \rightarrow$	* ↑ → Dies	ser PC → Lokaler Datenträger (C:) → \	Vindows > PolicyDefinitions		ٽ ~		
	diagnostics ^	Name	Änderungsdatum	Тур	Größe		^
	DiagTrack	DeviceInstallation.admx	05.12.2019 02:16	ADMX-Datei	15 KB		
	DigitalLocke	inetres.admx	05.12.2019 02:15	ADMX-Datei	1.672 KB		
	Downloade	MicrosoftEdge.admx	05.12.2019 02:14	ADMX-Datei	41 KB		
	en-US	Desktop.admx	19.03.2019 13:19	ADMX-Datei	14 KB		
	A Fonts	Logon.admx	19.03.2019 13:19	ADMX-Datei	11 KB		
	GameBarDre	AppHVSI.admx	19.03.2019 13:19	ADMX-Datei	12 KB		
	Clabaliatia	CredSsp.admx	19.03.2019 13:19	ADMX-Datei	14 KB		
	Globalizatio	EAIME.admx	19.03.2019 13:19	ADMX-Datei	8 KB		
	Help	MSDT.admx	19.03.2019 13:19	ADMX-Datei	6 KB		
	IdentityCRL	NetworkConnections.admx	19.03.2019 13:19	ADMX-Datei	17 KB		
	IME	EventLog.admx	19.03.2019 13:19	ADMX-Datei	15 KB		
	ImmersiveC	WCM.admx	19.03.2019 13:19	ADMX-Datei	5 KB		
	INF	appv.admx	19.03.2019 13:19	ADMX-Datei	35 KB		
	InputMetho	DiskQuota.admx	19.03.2019 13:19	ADMX-Datei	6 KB		
	1 2Cabamaa	📄 FileSys.admx	19.03.2019 13:19	ADMX-Datei	8 KB		
	L2Schemas	CM.admx	19.03.2019 13:19	ADMX-Datei	35 KB		
	LiveKernelR	iSCSI.admx	19.03.2019 13:19	ADMX-Datei	7 KB		
	Logs	🗋 Kerberos.admx	19.03.2019 13:19	ADMX-Datei	10 KB		
	Media	MSI.admx	19.03.2019 13:19	ADMX-Datei	17 KB		
	Microsoft.N	TaskScheduler.admx	19.03.2019 13:19	ADMX-Datei	6 KB		

Das ist ein guter Tag! Die Vorlagen haben sich zwischen Windows 10 Version 1903 und 1909 fast nicht verändert! Dennoch möchte ich hier meinen üblichen Zyklus darstellen. Bei einem Wechsel von 1809 auf 1909 wäre das definitiv erforderlich!

Ich verwende auf ADMX-Dateien für andere Anwendungen. Diese gehören nicht zum Betriebssystem-Standard. Damit ich von dem neuen Editor-Rechner die dazugehörigen Einstellungen verwalten kann, importiere ich die erforderlichen Dateien in das PolicyDefinitions-Verzeichnis. Hier kommen die Office-Templates, die SCT-SecurityTemplates und etwas Mozilla:

📕   🛃 📕 🖛   PolicyDefinitio	ons		o x	📙   🕑 📙 🖛   ADMX	- 0	×
Datei Start Freigeben	Ansicht		~ 🕐	Datei Start Freigeben Ansicht		~ 🕐
← → × ↑ 📙 « Wi →	Policy v Ö	PolicyDefinitions" durchsuchen		← → • ↑ 📴 « Zwis → ADMX 🔹 ♂	ADMX" durchsuchen	
Help ^ N	lame	Änderungsdatum	Тур ^	3D-Objekte ^ Name ^	Änderungsdatum	Тур
IdentityCRL	de-DE	05.12.2019 02:19	Dateiordn	Bilder de-de	29.12.2019 17:14	Dateior
IME	en-US	19.03.2019 13:16	Dateiordn	Desktop access16.admx	10.10.2019 01:27	ADMX-
ImmersiveC [	ActiveXInstallService.admx	19.03.2019 13:19	ADMX-Da	Dokumente AdmPwd.admx	31.10.2019 22:58	ADMX-
INF	AddRemovePrograms.admx	19.03.2019 13:19	ADMX-Da	Downloads	10.10.2019 01:27	ADMX-
InputMetho	AllowBuildPreview.admx	19.03.2019 05:46	ADMX-Da	Musik Direfox.admx	17.10.2018 13:20	ADMX-
12Schemas	AppCompat.admx	19.03.2019 13:19	ADMX-Da	Videos	10.10.2019 01:28	ADMX-
LiseKeenelD	AppHVSI.admx	19.03.2019 13:19	ADMX-Da	in Indes	01.03.2018 10:28	ADMX-
LiveKernelK	AppPrivacy.admx	19.03.2019 05:44	ADMX-Da	MSS-legacy.admx	31.10.2019 22:58	ADMX-
Logs	appv.admx	19.03.2019 13:19	ADMX-Da	DVD-Laufwerk office16.admx	10.10.2019 01:27	ADMX-
Media	AppxPackageManager.admx	19.03.2019 13:19	ADMX-Da	🛫 Freigaben (M:) 📄 onent16.admx	10.10.2019 01:27	ADMX-
Microsoft.N	AppXRuntime.admx	19.03.2019 05:46	ADMX-Da	📕 Zwischenabla 📄 outlk16.admx	10.10.2019 01:28	ADMX-
Migration	AttachmentManager.admx	19.03.2019 13:19	ADMX-Da	ADMX ppt16.admx	10.10.2019 01:27	ADMX-
minidump	AuditSettings.admx	19.03.2019 05:46	ADMX-Da	Windows 10 proj16.admx	10.10.2019 01:27	ADMX-
Modemillog	AutoPlay.admx	19.03.2019 05:46	ADMX-Da	Bibliotheken	10.10.2019 01:27	ADMX-
OCR	AVSValidationGP.admx	19.03.2019 05:44	ADMX-Da	SecGuide.admx	31.10.2019 22:58	ADMX-
OCK	Biometrics.admx	19.03.2019 05:46	ADMX-Da	teams16.admx	10.10.2019 01:27	ADMX-
to Offline Web	Bits.admx	19.03.2019 13:19	ADMX-Da	visio16.admx	10.10.2019 01:28	ADMX-
Panther	Camera.admx	19.03.2019 05:46	ADMX-Da	Papierkorb word16.admx	10.10.2019 01:27	ADMX-
Performanc	CEIPEnable.admx	19.03.2019 05:46	ADMX-Da	Windows 10 Vers		
PLA	CipherSuiteOrder.admx	19.03.2019 05:46	ADMX-Da 🗸	Documentation		
PolicvDefini 🗡 <			>	GP Reports V <		>
210 Elemente				18 Elemente		

Der Editor-PC ist einsatzbereit.

#### **GPO bereitstellen**

**IT-Solutions** 

Ich praktiziere das hier vorgestellte Modell seit einigen Versionen. Daher kann ich bereits auf bestehende Richtlinien zurückgreifen:

WS IT-Solutions

#### Gruppenrichtlinienobjekte in ws.its

ame	Objektstatus	WMI-Filter	Geändert	Besitzer
Default Domain Controllers Policy	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domän
Default Domain Policy	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domän
GPO-Benutzer	Computerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domän
GPO-Benutzer-Ordnerumleitung	Computerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domän
GPO-Benutzer-RDS	Computerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domän
GPO-Benutzer-Sicherheit-Office-2016	Computerkonfigurationseinstellungen d	Keine	15.11.2019 18:55:54	admin-setup (admin-setup@ws
GPO-Benutzer-Zertifikate	Computerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domär
GPO-Clients-RDS	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domär
GPO-Clients-Win10-1803-Datenschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1803	27.10.2019 17:32:42	Domänen-Admins (WS\Domär
GPO-Clients-Win10 <mark>-1803-Konfiguration</mark>	Benutzerkonfigurationseinstellungen d	Windows-10-1803	27.10.2019 17:32:40	Domänen-Admins (WS\Domär
GPO-Clients-Win10 <mark>-1803-Sicherheit</mark>	Benutzerkonfigurationseinstellungen d	Windows-10-1803	27.10.2019 17:32:42	Domänen-Admins (WS\Domär
GPO-Clients-Win10 <mark>-1903-Datenschutz</mark>	Benutzerkonfigurationseinstellungen d	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (WS\Domär
GPO-Clients-Win10 <mark>-1903-Konfiguration</mark>	Benutzerkonfigurationseinstellungen d	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Clients-Win10-1903-Konfiguration-PineAP	Benutzerkonfigurationseinstellungen d	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Clients-Win10 <mark>-1903-Sicherheit</mark>	Benutzerkonfigurationseinstellungen d	Windows-10-1903	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Benutzerprofile	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domä
GPO-Computer-MSRA	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Applocker	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Audit	Benutzerkonfigurationseinstellungen d	Keine	01.12.2019 16:54:18	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Audit-WEF	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Basics	Benutzerkonfigurationseinstellungen d	Keine	05.12.2019 17:45:24	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Bitlocker	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Cipher-TLS	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-DC	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Defender	Benutzerkonfigurationseinstellungen d	Windows-Server-2016	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-DeviceGuard	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Firefox	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Firewall	Benutzerkonfigurationseinstellungen d	Keine	25.11.2019 09:31:18	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-IExplore	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:40	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-LAPS-Clients	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-LAPS-Server	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:42	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-LSAProtection	Benutzerkonfigurationseinstellungen d	Keine	01.12.2019 17:05:20	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-Netzwerk	Benutzerkonfigurationseinstellungen d	Keine	27.10.2019 17:32:38	Domänen-Admins (WS\Domä
GPO-Computer-Sicherheit-NoNTLM	Benutzerkonfigurationseinstellungen d	Keine	05.12.2019 17:47:12	Domänen-Admins (WS\Domä

Ich habe für jede Betriebssystemversion 3 Gruppenrichtlinien für die Basiskonfiguration:

- GPO-<OSVersion>-Sicherheit
  - Diese GPO ist ein 1:1 Import der von Microsoft empfohlenen Security Baseline des Security Compliance Toolkits (SCT). Diese werden für jedes Betriebssystem herausgegeben.
  - Ich werde in dieser GPO keine Anpassungen vornehmen! Denn mit einem Wechsel auf ein neues Betriebssystem müsste ich herausfinden, welche Veränderungen ich vorgenommen hatte... Viel Spass dabei! Anpassungen kommen in die dritte GPO.
- GPO-<OSVersion>-Datenschutz
  - Die Security-Empfehlungen von Microsoft entsprechen nicht meinen Datenschutzanforderungen. Damit ich diese für Anforderungen aus der DSGVO und ähnlichen Regelwerken separat ausweisen kann, konfiguriere ich diese Einstellungen in einer separaten GPO.
- GPO-<OSVersion>-Konfiguration
  - Hier editiere ich alle funktionalen Einstellungen, wie z.B. die WSUS-Konfiguration
  - Auch Anpassungen des Betriebssystems gehören hier rein
  - Sollte eine Sicherheitseinstellung aus der SCT-Baseline zu streng oder zu schwach sein, dann platziere ich die Korrektur in dieser GPO

Wenn ihr heute auf dieses Schema umsteigen wollt, dann beginnt ihr mit leeren GPO. Wenn ihr aber nur für ein neues Betriebssystem erweitert (so wie ich hier in diesem WSHowTo), dann könnt ihr die bestehenden GPO kopieren und anpassen.

Ich benötige drei neue GPO. Die erste ist die einfachste, denn ihre Einstellungen importiere ich von der Microsoft-Baseline. Dafür benötige ich eine neue, leere GPO:

WS IT-Solutions



Die beiden anderen GPO (Konfiguration und Datenschutz) habe ich bereits in der Vorgängerversion. Für beide GPO kann ich also eine Kopie erstellen (wie gesagt: wer neu einsteigt, der muss 2 leere GPO erstellen und manuell befüllen):

/ 🔤 🚥			3	compation or ingeneration according on the	
✓      Gruppenrichtlinienobjekte		GPO-Benutzer-RDS		Computerkonfigurationseinstellungen d	Keine
Default Domain Controllers Policy		GPO-Benutzer-Sicherheit-Offic	e-2016	Computerkonfigurationseinstellungen d	Keine
Default Domain Policy		GPO-Benutzer-Zertifikate		Computerkonfigurationseinstellungen d	Keine
GPO-Benutzer		GPO-Clients-RDS		Benutzerkonfigurationseinstellungen d	Keine
GPO-Benutzer-Ordnerumleitung		GPO-Clients-Win10-1803-Date	enschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1803
GPO-Benutzer-RDS		GPO-Clients-Win 10-1803-Kon	iguration	Benutzerkonfigurationseinstellungen d	Windows-10-1803
GRO-Benutzer-Sicherheit-Office-2016		GPO-Clients-Win 10-1803-Sich	erheit	Benutzerkonfigurationseinstellungen d	Windows-10-1803
CPO Paratera Zatifilata		GPO-Clients-Win 10-1903-Date	enschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Benutzer-Zertinkate		GPO-Clients-Win 10-1903-Kon	iguration	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-KDS		GPO-Clients-Win 10-1903-Kon	iguration-PineAP	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1803-Datenschutz		GPO-Clients-Win10-1903-Sich	erheit	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1803-Konfiguration		GPO-Clients-Win 10-1909-Sich	erheit	Aktiviert	Keine
GPO-Clients-Win10-1803-Sicherheit		GPO-Computer-Benutzerprofile	•	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Datenschutz		GPO-Computer-MSRA		Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Konfiguratic	Pearbeiter		ocker	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Konfiguratic	DearDeiter			Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Sicherheit	Objektstat	tus >	-WEF	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1909-Sicherheit	Sichara		25	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Benutzerprofile	Sicherhan		cker	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-MSRA	Von Siche	rung wiederherstellen	er-TLS	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Applocker	Einstellun	igen importieren		Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Audit	Bericht sp	eichern	nder	Benutzerkonfigurationseinstellungen d	Windows-Server-2016
GPO-Computer-Sicherheit-Audit-WEF	benene sp		ceGuard	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Basics	Neues Fer	nster hier öffnen	ж	Benutzerkonfigurationseinstellungen d	Keine
GPO Computer Sicherheit Bitlecker	1.1.1		/all	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Bitlocker	Kopieren		ore	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Cipher-TL	Löschen		5-Clients	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-DC	Umbenen	nen	S-Server	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Defender			Protection	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-DeviceGua	Aktualisie	ren	werk	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Firefox	Hilfe		TLM	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Firewall			arShellWinRM	Benutzerkonfigurationseinstellungen d	Keine

WS IT-Solutions



GPO-Server-RDS     GPO-Server-RDS-Sicherheit-Applocker	
GPO-Server-RDS-Sicherheit-User	
GPO-Server-Win2016	
GPO-Server-Win2019-Datenschutz	
GPO-Server-Win2019-Konfiguration	
GPO-Server-Win2019-Sicherheit	
GPO-Clients-Win10-1909-Konfiguration	
> 🕞 WMI-Filter	
> 🛅 Starter-Gruppenrichtlinienobjekte	Hinzufügen Entfernen Eigenschaften
> 📫 Standorte	
🙀 Gruppenrichtlinienmodellierung	WMI-Filterung
	I Dieses Gruppenrichtlinienobiekt ist mit folgendem WMI-Filter verknüpft:

Für die Datenschutz-GPO erstelle ich nach dem gleichen Verfahren eine Kopie. Im Ergebnis sehe ich die drei neuen GPO:

/ 💼 🚥		comparation ingenetion reconcilingent a	
✓ → Gruppenrichtlinienobjekte	GPO-Benutzer-RDS	Computerkonfigurationseinstellungen d	Keine
Default Domain Controllers Policy	GPO-Benutzer-Sicherheit-Office-2016	Computerkonfigurationseinstellungen d	Keine
Default Domain Policy	GPO-Benutzer-Zertifikate	Computerkonfigurationseinstellungen d	Keine
GPO-Benutzer	GPO-Clients-RDS	Benutzerkonfigurationseinstellungen d	Keine
GPO-Benutzer-Ordnerumleitung	GPO-Clients-Win 10-1803-Datenschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1803
GPO-Benutzer-RDS	GPO-Clients-Win 10-1803-Konfiguration	Benutzerkonfigurationseinstellungen d	Windows-10-1803
GPO-Benutzer-Sicherheit-Office-2016	GPO-Clients-Win 10-1803-Sicherheit	Benutzerkonfigurationseinstellungen d	Windows-10-1803
GRO Reputzer Zertifikate	GPO-Clients-Win 10-1903-Datenschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Dendizer-Zentinkate	GPO-Clients-Win 10-1903-Konfiguration	Benutzerkonfigurationseinstellungen d	Windows-10-1903
	GPO-Clients-Win 10-1903-Konfiguration-PineAP	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1803-Datenschutz	GPO-Clients-Win 10-1903-Sicherheit	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1803-Konfiguration	GPO-Clients-Win 10-1909-Datenschutz	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1803-Sicherheit	GPO-Clients-Win 10-1909-Konfiguration	Benutzerkonfigurationseinstellungen d	Windows-10-1903
GPO-Clients-Win10-1903-Datenschutz	GPO-Clients-Win 10-1909-Sicherheit	Aktiviert	Keine
GPO-Clients-Win10-1903-Konfiguration	GPO-Computer-Benutzerprofile	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Konfiguration-Pin	eAP GPO-Computer-MSRA	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1903-Sicherheit	GPO-Computer-Sicherheit-Applocker	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1909-Datenschutz	GPO-Computer-Sicherheit-Audit	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1909-Konfiguration	GPO-Computer-Sicherheit-Audit-WEF	Benutzerkonfigurationseinstellungen d	Keine
GPO-Clients-Win10-1909-Sicherheit	GPO-Computer-Sicherheit-Basics	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Benutzerprofile	GPO-Computer-Sicherheit-Bitlocker	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-MSRA	GPO-Computer-Sicherheit-Cipher-TLS	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Applocker	GPO-Computer-Sicherheit-DC	Benutzerkonfigurationseinstellungen d	Keine
GPO-Computer-Sicherheit-Audit	GPO-Computer-Sicherheit-Defender	Benutzerkonfigurationseinstellungen d	Windows-Server-2016
GPO-Computer-Sicherheit-Audit-WEE	GPO-Computer-Sicherheit-DeviceGuard	Benutzerkonfigurationseinstellungen d	Keine
a of o compater bienement Addit Wer	GPO-Computer-Sicherheit-Firefox	Benutzerkonfigurationseinstellungen d	Keine

Damit diese Richtlinien nur von Clients mit Windows 10 Version 1909 verarbeitet werden, benötige ich einen WMI-Filter. Auch hier kann ich einen Vorgänger kopieren. Wichtig ist die WMI-Abfrage – man kann also auch einfach einen neuen Filter ohne Kopie erstellen:



Nach dem Umbenennen passe ich den Filter an. Die Versionsnummer lese ich mit winver.exe aus:

📓 Gruppenrichtlinienverwaltung		– 🗆 X
🛣 Datei Aktion Ansicht Fenster ?		- 8
🗢 🔿 🔁 🔚 🗙 🖸 🔢 🖬		
Gruppenrichtlinienverwaltung	Windows-10-1909         Aligemein       Delegierung         WMI-Filter         Beschreibung:         Abfragen:         Namespace         root\CIMv2	Abfrage       Abfrage         select * from Win32_OperatingSystem where Version like **10.0.18362** and ProductType=1          die diesen WMI-Filter verwenden
> i Starter-Gruppenrichtlinienobjekte	Folgende Gruppenrichtlinienobje	kte sind mit diesem WMI-Filter verknüpft:
Coppendictanterverwarding     Datei Aktion Ansicht Fenster ?     Datei Aktion Ansicht Fenster ?     Description Compensional Compensinterve Compensional Compensional Co	×	
		Filter bearbeiten.
Abfragen:     Apfragen:     Apfrage     Apfrage	em where uctType=1 Entfemen Bearbeiten	select * from Win32_DperatingSystem where Version like "10.0.18362" and ProductType=1
> 📸 Standor	Speichem Abbrect roo	II-Abfrage × mespace: \/CIMv2 Durchsuchen
R Gruppenrichtlinienergebnisse	Abf sei an	rage: ect * from Win32_Operating System where Version like "10.018363" froductType=T OK Abbrechen

Jetzt kann ich den neuen WMI-Filter den neuen GPO zuweisen:

WS IT-Solutions

WS IT-Solutions

## WSHowTo – moderne GPO-Versionierung am Beispiel Windows 10 2020-01-30 Gruppenrichtlinien



Jetzt sind die GPO bereit für den inhaltlichen Abgleich:



#### GPO Sicherheit (SCT-Baseline)

Die Sicherheitseinstellungen empfiehlt Microsoft für jede Betriebssystemversion. Die Qualität der Empfehlungen schwankt durchaus. Daher sollte man die Einstellungen immer testen. Man sucht die neusten Releases online. Achtet hier bitte auf die Quelle der Informationen: die Seite sollte schon von Microsoft kommen:



security compliance toolkit Q
Web Bilder Videos Nachrichten Karten Einstellungen •
Deutschland * Sichere Suche: Moderat * Irgendwann *
Download Microsoft Security Compliance Toolkit 1.0 from https://www.microsoft.com/en-us/download/details.aspx?id=55319 21. Nov. 2019 - This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.
Microsoft Security Compliance Toolkit 1.0 - Windows security thtps://docs.microsoft.com/en-us/windows/security/threat-protection/security-complia Microsoft Security Compliance Toolkit 1.0. 11/21/2019; 2 minutes to read +2; In this article What is the Security Compliance Toolkit (SCT)? The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products.
Compliance Toolkit I Security Health Plan  thtps://www.securityhealth.org/brokers/compliance-toolkit  The Toolkit provides compliance and privacy training information for Security Health Plan's First tier, Downstream and Related entities (FDRs) to enter into or maintain a business relationship.

Der anschließende Download ist einfach. Achtet bitte auf das Release-Datum und eventuelle "Drafts" (Entwürfe):

www.microsoft.com/en-us/download/details	aspx?id=55319	
Microsoft Security Complian	ce Toolkit 1.0	
Important! Selecting a language below Language: <b>English</b>	will dynamically change the complete page	e content to that language. Download
This set of tools allows enterp edit and store Microsoft-reco and other Microsoft products	rise security administrators to mmended security configurat while comparing them again	o download, analyze, test, tion baselines for Windows nst other security
Details		
Note: There are multiple files availab to select the files you need.	e for this download. Once you click on the "	'Download" button, you will be prompted
Version: 1.0	Dat 11/2	e Published: 1 <mark>/2</mark> 019
File Name:	File	Size:

In dem ZIP-Archiv befinden sich etliche Unterordner. Der Ordner "GPO" enthält die exportieren Richtlinien:





Diese Exports kann man nun einfach importieren:



Nach der Auswahl des Verzeichnisses sieht man die einzelnen GPO mit ihrem Namen. Mein Zielsystem ist ein Client. Daher wähle ich diese Richtlinie aus:



Importeinstellungen-Assistent X	×
Wall-GPO Wählen Sie ein Gruppenrichtlinienobjekt aus, von dem Sie Einstellungen importieren möchten.	-Win10-1909-Sicherheit
Gesicherte Gruppenrichtlinienobjekte:	s Einstellungen Delegierung Status
Name Zetstempel A	lients-Win 10-1909-Sicherheit tet am. 29.12.2019 15.36.12 Alle einblenden
MSFT Internet Explorer 11 - User 12.11.2019 01:3 MSFT Windows 10 1909 - BitLocker 12.11.2019 01:3	Ausblenden
MSFT Windows 10 1909 - Computer         12.11.2019 01:3           Image: MSFT Windows 10 1909 - User         12.11.2019 01:3	s Einblenden
<ul> <li>MSFT Windows 10 1909 and Server 1909 - Defender Ant 12.11.2019 01:3</li> <li>MSFT Windows 10 1909 and Server 1909 - Domain Sec 12.11.2019 01:3</li> </ul>	uptungen <u>Einblenden</u>
C >	Einblenden
Version anzeigen	erung
< Zurück Weiter > Abbrechen Hilfe	konfiguration (Aktiviert)
GPO-Clients-Win10-1803-Konfiguration	Keine Einstellungen definiert

Wenige Klicks später ist der Export in die leere GPO importiert:

K Gruppenrichtlinienverwaltung		- 🗆 X
📠 Datei Aktion Ansicht Fenster ?		- 8
Gruppenrichtlinienverwaltung	GPO-Clients-Win10-1909-Sicherheit	
✓ A Gesamtstruktur: ws.its	Remich Detaile Finstellungen Delegienung Statue	
🗸 📑 Domänen		
V 🟥 ws.its	GPO-Clients-Win10-1909-Sicherheit	
🛒 Default Domain Policy	Daten emittelt am: 29.12.2019 15:39:04	Alle einblenden
> 📓 Domain Controllers		, no emprendent
> Microsoft Exchange Security Groups		Ausblenden
> II WS	Details	
Gruppenrichtlinienobjekte		Einblenden
Default Domain Controllers Policy     Pefault Demain Peliau	Verknüpfungen	Finblandan
GPO-Beputzer	Sicherheitsfilten nn	
GPO-Benutzer-Ordnerumleitung	or a new of the second s	Einblenden
GPO-Benutzer-BDS	WMI-Filterung	
GPO-Benutzer-Sicherheit-Office-2016		Einblenden
GPO-Benutzer-Zertifikate	Delegierung	Finblandan
GPO-Clients-RDS	Computed configuration (Altiviat)	
GPO-Clients-Win10-1803-Datenschutz		Ausblenden
GPO-Clients-Win10-1803-Konfiguration	Richtlinien	
GPO-Clients-Win10-1803-Sicherheit		Ausblenden
GPO-Clients-Win10-1903-Datenschutz	windows-Einstellungen	Ausblenden
GPO-Clients-Win10-1903-Konfiguration	Sicherheitseinstellungen	
GPO-Clients-Win10-1903-Konfiguration-PineAP		Einblenden
GPO-Clients-Win10-1903-Sicherheit	Administrative Vorlagen	Finblandan
GPO-Clients-Win I0- 1909-Datenschutz	Poputandroafiguration (Dealdiviat)	Linbienden
GPO-Clients-Win10-1909-Konfiguration		Ausblenden
GPO-Computer-Reputzerprofile	Keine Einstellungen definiert	
GPO-Computer-MSRA		
GPO-Computer-Sicherheit-Applocker		
GPO-Computer-Sicherheit-Audit		
GPO-Computer-Sicherheit-Audit-WEF		
GPO-Computer-Sicherheit-Basics		

Ich kommentiere gerne die Richtlinien. Daher öffne ich die neue GPO mit dem Editor:

📓 Gruppenrichtlinienverwaltung	- 🗆 X
📠 Datei Aktion Ansicht Fenster ?	- <i>6</i>
🗢 🔿 📶 🖻 İ 🗙 🔍 📓 🗊	
<ul> <li>Gruppenrichtlinienobjekte</li> <li>Default Domain Controllers Policy</li> <li>Default Domain Policy</li> <li>GPO-Benutzer</li> </ul>	GPO-Clients-Win10-1909-Sicherheit Bereich Details Einstellungen Delegierung Status Verknüpfungen
GPO-Benutzer-Ordnerumleitung	Fur dieses Verzeichnis anzeigen: ws.its
GPO-Benutzer-Robs GPO-Benutzer-Sicherheit-Office-2016 GPO-Benutzer-Zertifikate GPO-Clients-RDS GPO-Clients-Win10-1803-Datenschutz GPO-Clients-Win10-1803-Sicherheit GPO-Clients-Win10-1803-Jatenschutz GPO-Clients-Win10-1903-Jatenschutz	Die tolgenden Standorte, Domanen und Organisationseinheiten sind mit dem Objekt verknuptt:           Pfad                Pfad               Pfad               Pfad               Pfad               Pfad
GPO-Clients-Win10-1903-Konfiguration-PineAP  GPO-Clients-Win10-1903-Sicherheit  GPO-Clients-Win10-1909-Datenschutz  GPO-Clients-Win10-1909-Configuration	Sicherheitsfilterung Die Einstellungen dieses Gruppenichtlinienobjekts gelten nur für die folgenden Gruppen, Benutzer und Computer:
GPO-Computer-MSRA GPO-Computer-Scherheit-Apploc GPO-Computer-Scherheit-Apploc Scherheit-Apploc	nu. atus >>
GPO-Computer-Sicherheit-Audit-V Von Sich	erung wiederherstellen naen importieren Entlemen Bgenschaften

WS IT-Solutions

WSHowTo – moderne GPO-Versionierung am Beispiel Windows 10 2020-01-30 Gruppenrichtlinien

In den Eigenschaften geht es weiter:



Hier vermerke ich mir genau die Informationen der originalen GPO mit dem dazugehörigen Release-Date. Falls es später eine neue Version gibt, kann ich das eindeutig nachvollziehen. Das Datum und den Namen übernehme ich aus dem "Quell-Import"-Dialog des Importes:

Gruppenrichtlinienverwaltungs-Editor		_	$\times$
Datei Aktion Ansicht ?			
🗢 🌩   💼   🖬 🗟 🖬	Eigenschaften von GPO-Clients-Win10-1909-Sicherhei ? X		
GPO-Clients-Win10-1909-Sicherheit [WS-DC1.WS.ITS] Ri  Computerkonfiguration  Richtlinien  Sinstellungen  Kinstellungen  Kinst	Allgemein Verknüpfungen Sicherheit Kommentar GPO-Clients-Win 10-1909-Sicherheit [WS-DC1.WS.ITS]		
> 📑 Richtlinien > 🗎 Einstellungen	Kommentar 2019-12-29 Stephan Walther - Import der SCT-Baseline "MSFT Windows 10 1909 - Computer" vom 12.11.2019 01.30.04		

An der Computerversion kann ich genau erkennen, dass diese GPO nach dem Import nicht verändert wurde. Jede Anpassung würde den Zähler nach oben korrigieren:



Damit wäre die erste GPO einsatzbereit – von einer Testphase mal abgesehen.

#### <u>GPO Datenschutz</u>

Die zweite GPO ist eine Kopie der Vorgänger-Richtlinie für Windows 10 Version 1903. Für mich sind hier 2 grundsätzliche Aktionen wichtig:

- Ich muss nach nicht mehr kompatiblen Einstellungen suchen und diese für 1909 entfernen
- Ich muss aber auch nach neuen Einstellungen suchen, die es für 1903 noch nicht gab.

Beides erreiche ich, indem ich die GPO mit einem Editor-Rechner bearbeite, der die neuen Vorlagen verwendet. Inkompatible Einstellungen finde ich unter "Extra Registry Settings". Hier seht ihr ein Beispiel für eine Problem-GPO:

K Gruppenrichtlinienverwaltung		>
属 Datei Aktion Ansicht Fenster ?		- 5
← ⇒   22 📰 🔍 📓 🗊		post of the second s
GPO-Clients-Win10-1909-Konfiguration	GPO-Computer-Sicherheit-Defender	
GPO-Clients-Win10-1909-Sicherheit  GPO-Computer-Benutzerprofile  GPO-Computer-MSRA	Bereich Details Einstellungen Delegierung Status	
GPO-Computer-Sicherheit-Applocker	GPO-Computer-Sicherheit-Detender	
GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Audit-WEF	Algemein	Enblenden
GPO-Computer-Sicherheit-Bitlocker  GPO-Computer-Sicherheit-Cinher-II S	Computerkonfiguration (Aktiviert)	Ausblenden
GPO-Computer-Sicherheit-DC	Administrative Vorlagen	Ausblenden
GPO-Computer-Sicherheit-DeviceGuard	Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.	Ausblenden
GPO-Computer-Sicherheit-Firewall	Windows-Komponenten/Windows Defender Antivirus	Enblenden
GPO-Computer-Sicherheit-LAPS-Clients	Windows-Komponenten/Windows Defender Antivirus/Echil2elischul2 Windows-Komponenten/Windows Defender Antivirus/MAPS	Enblenden
GPO-Computer-Sicherheit-LSAProtection	Windows-Komponenten/Windows Defender Antivirus/Scan	Einblenden
GPO-Computer-Sicherheit-NoNTLM	Zusätzl. Regeinst.	Ausblenden
GPO-Computer-Sicherheit-Scope-Clients-JB GPO-Computer-Sicherheit-Scope-Clients-Standard	Für einige Einstellungen konnten keine Anzeigenamen gefunden werden. Eine Aktua verwendeten ADM-Dateien behebt möglicherweise das Problem.	slisierung der von der Gruppenrichtlinienverwaltung
GPO-Computer-Sicherheit-Scope-Clients-WSITS	Einstellung Status	
GPO-Computer-Sicherheit-Scope-Server-HyperV GPO-Computer-Sicherheit-Scope-Server-JB GPO-Computer-Sicherheit-Scope-Server-Monitorin	Software \Policies\Microsoft\Windows 1 Defender\MpEngine\MpEnablePus	
GPO-Computer-Sicherheit-Scope-Server-MX GPO-Computer-Sicherheit-Scope-Server-RDS	Benutzerkonfiguration (Deaktiviert)	Ausblenden
GPO-Computer-Sicherheit-Scope-Server-Standard	Keine Einstellungen definiert	
GPO-Computer-Sicherheit-Scope-Zero		

Fehlt dieser Punkt, dann besteht eine gute Chance auf Kompatibilität:

WS IT-Solutions

📓 Gruppenrichtlinienverwaltung		- 0	×			
🔜 Datei Aktion Ansicht Fenster ?		1	- & ×			
Gruppenrichtlinienobjekte	GPO-Clients-Win10-1909-Datenschutz					
Default Domain Controllers Policy     Default Domain Policy     GPO-Benutzer	Bereich Details Einstellungen Delegierung Status		_			
GPO-Benutzer-Ordnerumleitung	GPO-Clients-Win10-1909-Datenschutz GPO-Benutzer-Ordnerumleitung Daten emittet am: 29.12.2019 15:53:41					
GPO-Benutzer-Sicherheit-Office-2016  GPO-Benutzer-Zotifikate	Allgemein	Einblenden	_			
GPO-Clients-RDS	Computerkonfiguration (Aktiviert)	Ausblenden				
GPO-Clients-Win10-1803-Datenschutz	Richtlinien	Ausblenden				
GPO-Clients-Win10-1803-Sicherheit GPO-Clients-Win10-1903-Datenschutz	Administrative vonagen	Ausblenden				
GPO-Clients-Win10-1903-Konfiguration GPO-Clients-Win10-1903-Konfiguration-PineAP	System/Benutzerprofile	Deblesdes				
GPO-Clients-Win10-1903-Sicherheit	Systemsteuerung/Regions- und Sprachoptionen/Handschriftanpassung	Enblenden				
GPO-Clients-Win10-1909-Konfiguration	Windows-Komponenten/Anwendungskompatibilität	Einblenden				
GPO-Computer-Benutzerprofile	Windows-Komponenten/App-Datenschutz	Einblenden				
II GPO-Computer-MSRA II GPO-Computer-Sicherheit-Applocker	Windows-Komponenten/App-Laufzeit	Einblenden				
GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Audit-WEF	Windows-Komponenten/Audiorecorder	Einblenden				
GPO-Computer-Sicherheit-Basics	Windows-Komponenten/Cloudinhalt	Einblenden				
GPO-Computer-Sicherheit-Cipher-TLS	Windows-Komponenten/Datensammlung und Vorabversionen	Enblenden	_			
GPO-Computer-Sicherheit-DC GPO-Computer-Sicherheit-Defender	Windows-Komponenten/Einstellungen suschmpisiaren	Einblenden				
GPO-Computer-Sicherheit-DeviceGuard GPO-Computer-Sicherheit-Firefox	Windows-Komponenten/Internet Explorer/Sicherheitsfunktionen	Einblenden				
GPO-Computer-Sicherheit-Firewall	Windows-Komponenten/Karten	Einblenden	~			
I GPU-Computer-Sicherheit-IExplore ♥		Einblenden				

📓 Gruppenrichtlinienverwaltung		- 🗆 X
📓 Datei Aktion Ansicht Fenster ?		- 8
🗢 🔿 🙍 📰 🙆 🔢 🖬		I
✓ i Gruppenrichtlinienobjekte	GPO-Clients-Win10-1909-Datenschutz	
Default Domain Controllers Policy	Bereich Details Einstellungen Delegierung Status	
Default Domain Policy     GRO D		Finblenden
GPO-Benutzer	Windows-Komponenten/Datensammlung und Vorabversionen	
GPO-Benutzer-Ordnerumieitung		Einblenden
GPO-Benutzer-Sicherheit-Office-2016	Windows-Komponenten/Digitalschließfach	Finblenden
GPO-Benutzer-Zertifikate	Windows-Komponenten/Einstellungen synchronisieren	Lindenden
GPO-Clients-RDS		Einblenden
GPO-Clients-Win10-1803-Datenschutz	Windows-Komponenten/Internet Explorer/Sicherheitsfunktionen	Enblandan
GPO-Clients-Win10-1803-Konfiguration	Windows-Komponenten/Karten	Linblenden
GPO-Clients-Win10-1803-Sicherheit		Einblenden
GPO-Clients-Win10-1903-Datenschutz	Windows-Komponenten/Mein Gerät suchen	Cablesdee
GPO-Clients-Win10-1903-Konfiguration	Windowe-Komponenten /Nachrichten	Enbienden
GPO-Clients-Win10-1903-Konfiguration-PineAP	Windows-Komponenten/ Nacimenten	Einblenden
GPO-Clients-Win10-1903-Sicherheit	Windows-Komponenten/OneDrive	
GPO-Clients-Win10-1909-Datenschutz		Einblenden
GPO-Clients-Win10-1909-Konfiguration	windows-komponenten/Unlineunterstutzung	Einblenden
GPO-Clients-Win10-1909-Sicherheit	Windows-Komponenten/Suche	
GPO-Computer-Benutzerprofile		Einblenden
GPO-Computer-MSRA	Windows-Komponenten/Texteingabe	Finblenden
GPO-Computer-Sicherheit-Applöcker	Windows-Komponenten/Übermittlungsoptimierung	
GPO-Computer-Sicherheit-Audit		Einblenden
GPO-Computer-Sicherheit-Rasics	Windows-Komponenten/Windows Defender Antivirus/MAPS	Finblenden
GPO-Computer-Sicherheit-Bitlocker	Windows-Komponenten/Windows Defender SmartScreen/Explorer	Lindenden
GPO-Computer-Sicherheit-Cipher-TI S		Einblenden
GPO-Computer-Sicherheit-DC	Windows-Komponenten/Windows-Fehlerberichterstattung	Debles des
GPO-Computer-Sicherheit-Defender	Windows Kompanantan Mindows Spielzyfreiden und übertergung	Einblenden
GPO-Computer-Sicherheit-DeviceGuard		Einblenden
GPO-Computer-Sicherheit-Firefox	Benutzerkonfiguration (Deaktiviert)	
GPO-Computer-Sicherheit-Firewall		Ausblenden
GPO-Computer-Sicherheit-IExplore	Keine Einstellungen definiert	~

Sehr gut: Der zusätzliche Punkt fehlt. Natürlich kann es jetzt immer noch zu den Problemen wie in den Szenarien 2 und 3 kommen. Aber diese kann ich anders prüfen. Dazu später mehr.

Weiter geht es in der Kommentar-Sektion. Hier sollte eine Quellenangabe platziert werden:

VS IT-Solutions

Gruppenrichtlinienverwaltungs-Editor		_	×
<ul> <li>GPO-Clients-Win10-1909-Datenschutz [WS-DC1</li> <li>Computerkonfiguration</li> <li>Citchinien</li> <li>Citchinien</li> <li>Einstellungen</li> <li>Benutzerkonfiguration</li> <li>Citchinien</li> <li>Einstellungen</li> <li>Einstellungen</li> </ul>	GPO-Clients-Win10-1909-Datenschutz [WS-DC1.WS.ITS] Richtlinie  Markieren Sie ein Element, um dessen Name Beschreibung anzuzei Eigenschaften von GPO-Clients-Win10-1909-Datensch?  Algemein Verknüpfungen Sicherheit Kommentar  GPO-Clients-Win10-1909-Datenschutz [WS-DC1.WS.ITS] Kommentar  2019-12-30 Stephan Wather - Kopie von "GPO-Clients-Win10-1903-Datenschutz"		

Und im nächsten Schritt gehe ich alle Einstellungen mit dem Editor durch und suche nach zusätzlichen Einstellungen zum Datenschutz. Hier kann natürlich auch eine Internet-Recherche helfen. Ich finde ein paar Einstellungen, die ich vorher noch nicht konfiguriert hatte. Das hole ich nun nach:

Gruppenrichtlinienverwaltungs-Editor				_	×
Datei Aktion Ansicht ?					
🗢 🔿 🔁 🚾 🔒 🖬 🖬 🔺 🍸					
GPO-Clients-Win10-1909-Datenschutz [WS-DC1.V ^	📔 Betriebssystemrichtlinien				
Computerkonfiguration     Bichtlinien	Synchronisierung der	Einstellung	Status	Kommentar	
> Softwareeinstellungen	Zwischenablage geräteübergreifend	📰 Zwischenablageverlauf zulassen	Nicht konfigur	Nein	
> 📋 Windows-Einstellungen	Zulassen	Synchronisierung der Zwischenablage geräteübergreifend z…	Deaktiviert	Nein	
🗸 🚞 Administrative Vorlagen: Vom Iokalen C	Richtlinieneinstellung bearbeiten	🗈 Aktivitätsfeed aktivieren	Deaktiviert	Nein	
Crucker		📔 Veröffentlichen von Benutzeraktivitäten zulassen	Deaktiviert	Nein	
> 📫 Netzwerk	Anforderungen: Mindestens Windows Server 2016	📔 Upload von Benutzeraktivitäten zulassen	Deaktiviert	Nein	
Server	Windows 10				
> 🧮 Startmenü und Taskleiste					
V 🔛 System	Beschreibung:				
Anmelden	Diece Richtlinieneinstellung				
Antischadsoftware-Frühstart	legt fest, ob der Inhalt der				
Anzeige	Zwischenablage geräteübergreifend				
> App-v	synchronisiert werden kann.				
Beputzerprofile	Richtlinieneinstellung aktivieren				
Betriebssystemrichtlinien	dürfen Inhalte der Zwischenablage				
Dateiklassifizierungsinfrastruktu	auf Geräten synchronisiert werden,				
	I die unter demselben Microsoft-Konto				

Die Datenschutzeinstellungen können durchaus etwas Zeit in Anspruch nehmen. Gerade in Umgebungen mit Cloud-Anbindung ist hier Fingerspitzengefühl gefragt. Microsoft hat beim Datenschutz einfach eine wenig deutsche Mentalität...

#### GPO Konfiguration

Weiter geht es mit der dritten GPO. Das Vorgehen entspricht dem der Datenschutz-GPO. Ich habe auch hier wenig zu tun: Es gibt keine verwaisten Einstellungen und neue Elemente sind auch nicht dazu gekommen. Der Wechsel von Windows 10 1903 nach 1909 ist sehr einfach. Das muss aber nicht so sein.



#### Kompatibilität sonstiger GPO

Wie man vielleicht im oberen Bild erkennen kann, verwende ich momentan nicht durchgängig das Modell mit den drei Gruppenrichtlinien je Betriebssystem. Ich habe dazu noch etliche versionsübergreifende GPO. Damit kann ich Einstellungen relativ einfach einzeln zurücknehmen (für das TroubleShooting). Aber bei einem Versionswechsel muss ich auch jede einzeln auf Kompatibilität prüfen. Das sind meine GPO:

Datei Aktion Ansicht Fenster ?					
• 🔿 🔁 🚾   🙆 🖬					
	Clients Verknüpfte Gruppe Die Liste enthält k	enrichtlinienobjekte Gruppenrichtlinienverefbung Dek eine mit Standorten verknüpften Gruppenrichtlinienobjek	egierung te. Weitere Informatione	en erhalten Sie in der Hilfe.	WMLEther
GPO-Clients-RDS		GPO-Computer-MSRA	Clients	Benutzerkonfigurations	Keine
GPO-Clients-Win10-1803-Datenschutz GPO-Clients-Win10-1803-Konfiguration GPO-Clients-Win10-1803-Konfiguration GPO-Clients-Win10-1903-Sonfiguration GPO-Clients-Win10-1903-Sonfiguration GPO-Clients-Win10-1903-Konfiguration GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Baiscs GPO-Computer-Sicherheit-Baiscs GPO-Computer-Sicherheit-Baiscs GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-Firefox GPO-Computer-Sicherheit-IsDaPore GPO-Computer-Sicherheit-IsDa	2 3 3 6 6 7 6 8 9 0 10 11 12 13 14 15 16 17 8 19 20 21 22	GPO-Computer-Sicherheit-UAC-light GPO-Computer-Sicherheit-UAC-light GPO-Computer-Sicherheit-Apploxker GPO-Computer-Sicherheit-SAPtotection GPO-Computer-Sicherheit-LSAPtotection GPO-Computer-Sicherheit-Basics GPO-Computer-Sicherheit-APS-Clients GPO-Computer-Sicherheit-APS-Clients GPO-Computer-Sicherheit-APS-Clients GPO-Computer-Sicherheit-APS-Clients GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Audit GPO-Computer-Sicherheit-Apoles GPO-Computer-Sicherheit-Floore GPO-Computer-Sicherheit-Floore GPO-Computer-Sicherheit-Floore GPO-Clients-Win 10-1803-Datenschutz GPO-Clients-Win 10-1803-Sicherheit GPO-Clients-Win 10-1803-Sicherheit GPO-Clients-Win 10-1803-Sicherheit GPO-Clients-Win 10-1803-Sicherheit GPO-Clients-Win 10-1803-Sicherheit GPO-Clients-Win 10-1803-Sicherheit Default Domain Policy	Cierts Ci	Benutzekorfigurations Benutzekorfigurations	Keine Keine

Die Validierung nehme ich direkt in der Gruppenrichtlinien-Verwaltungskonsole vor. Dazu selektiere ich eine GPO und prüfe die Anzeige in den Einstellungen. Finde ich einen "zusätzlichen Registry-Eintrag", dann prüfe ich dessen Ursprung genau. Dieser gehört zu einer bekannten Extension: Dem Bitlocker-Network-Unlock. Dieser wird hier generell nicht richtig angezeigt. Gleichzeitig bestehen aber keine Kompatibilitätsprobleme

📓 Gruppenrichtlinienverwaltung			- 0	×
🔜 Datei Aktion Ansicht Fenster ?				- 8 ×
🗢 🔿 📶 🙆 🛛 🖬				
	000.00	unuden Sinh als id Bidla dans		
GPO-Clients-RDS	GPO-Con	nputer-sicherheit-Bitlocker		
GPO-Clients-Win10-1803-Datenschutz	Bereich L	Jetails Einstellungen Delegierung		
GPO-Clients-Win10-1803-Konfiguration	CPC	Computer-Sicherheit-Bitlacker		
GPO-Clients-Win10-1803-Sicherheit	Daten	emittelt am: 29 12 2019 17:16:40	Alle einblenden	
GPO-Clients-Win10-1903-Datenschutz	Allger	nein		
GPO-Clients-Win10-1905-Kontiguration			Einblenden	
GPO-Computer-MSRA	Comp	uterkonfiguration (Aktiviert)	Ausblanden	
GPO-Computer-Sicherheit-Applocker	Rich	htlinien	Ausbiertuer	
GPO-Computer-Sicherheit-Audit			Ausblenden	
GPO-Computer-Sicherheit-Basics	Ac	dministrative Vorlagen	Ausblenden	
GPO-Computer-Sicherheit-Bitlocker		Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Comput	ter abgerufen.	
GPO-Computer-Sicherheit-DeviceGuard		Windows-Komponenten/BitLocker-Laufwerkverschlüsselung/	Betriebssystemlaufwerke	
GPO-Computer-Sicherheit-Firefox			Einblenden	
GPO-Computer-Sicherheit-Firewall		windows-komponenten/bit Locker-Laurwerkverschlusselung/	Einblenden	
GPO-Computer-Sicherheit-IExplore		Windows-Komponenten/BitLocker-Laufwerkverschlüsselung/	Wechseldatenträger	
GPO-Computer-Sicherheit-LAPS-Clients		Zusätzi Reg -einst	Einbienden	
GPO-Computer-Sicherheit-LSAProtection			Ausblenden	
GPO-Computer-Sicherheit-PowerShellWinRM		Für einige Einstellungen konnten keine Anzeigenamen gefunden we verwendeten ADM-Dateien beheht möglicherweise das Problem	rden. Eine Aktualisierung der von der Gruppenrichtlinienverwaltung	
GPO-Computer-Sicherheit-SmartCard				
GPO-Computer-Sicherheit-UAC-light		Einstellung	Status	
GPO-Computer-Sicherheit-Zertifikate		SOFTWARE\Policies\Microsoft\SystemCertificates\FVE_NKP\C	Ausgestellt für	
> 📓 Clients-JB		ertificates\6CAA8BAA10A76F39AAF5B3088CAE81C73790E948	BitlockerNetworkUnlock	
> Clients-Standard		\Blob	Ausgestellt von WS-ITS-Zettifizien ingsstelle-CA1	
E Exchange-Objekte			Ablaufdatum	
> Gruppen			06.04.2020 08:59:43	
> 📓 Server			Beabsichtigte Zwecke	
> 📑 Gruppenrichtlinienobjekte			BitLocker-Laufwerkverschlüsselung	
> 😫 WMI-Filter				~

Gleiches gilt für die automatische Zertifikat-Verteilung. Die ist unproblematisch:

WS IT-Solutions



Alle anderen GPO werden korrekt angezeigt und sind damit kompatibel. Nur die Defender-GPO spielt nicht mit. Diese muss ich separat editieren:

📓 Gruppenrichtlinienverwaltung			- 🗆 X
📓 Datei Aktion Ansicht Fenster ?			- 8
GPO-Clients-Win10-1909-Konfiguration	GPO-C	computer-Sicherheit-Defender	
GPO-Clients-Win10-1909-Sicherheit	Bereich	Netails Einstellungen Delegiening Status	
GPO-Computer-Benutzerprofile	Dereicit	Decails and the spin belogicaling Status	
GPO-Computer-MSRA		PO-Computer-Sicherheit-Defender	
GPO-Computer-Sicherheit-Applocker		aten emittelt am: 29 12 2019 15:55:42	Alle einblenden
GPO-Computer-Sicherheit-Audit			The emplement
GPO-Computer-Sicherheit-Audit-WEF	///	gemein	Einblenden
GPO-Computer-Sicherheit-Basics	Co	mputerkonfiguration (Aktiviert)	
GPO-Computer-Sicherheit-Bitlocker			Ausblenden
GPO-Computer-Sicherheit-Cipher-ILS	7	lichtlinien	Austriandan
GPO-Computer-Sicherheit-DC		Administrative Vorlageo	Ausbienden
GPO-Computer-Sicherheit-Derender			Ausblenden
GPO-Computer-Sicherheit-DeviceGuard		Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.	
GPO-Computer-Sicherheit-Firewall		Windows-Komponenten/Windows Defender Antivirus	
GPO-Computer-Sicherheit-IExplore		Windows Komponenten Windows Defender Antivirus (Febtzeitschutz	Einblenden
GPO-Computer-Sicherheit-LAPS-Clients		Windows-Komponenten/ Windows Derender Antivirds/Echildender	Einblenden
GPO-Computer-Sicherheit-LAPS-Server		Windows-Komponenten/Windows Defender Antivirus/MAPS	
GPO-Computer-Sicherheit-LSAProtection			Einblenden
GPO-Computer-Sicherheit-Netzwerk		Windows-Komponenten/Windows Defender Antivirus/Scan	Einblenden
GPO-Computer-Sicherheit-NoNTLM		Zusätzl. Regeinst.	
GPO-Computer-Sicherheit-PowerShellWinRM			Ausblenden
GPO-Computer-Sicherheit-Scope-Clients-JB		Für einige Einstellungen konnten keine Anzeigenamen gefunden werden. Eine Aktualisierung der von verwendeten ADM-Dateien beheht mönlicherweise das Problem	der Gruppenrichtlinienverwaltung
GPO-Computer-Sicherheit-Scope-Clients-Standard		Verwerkdeten Abhr-Dateien berebt möglicherweide das Froblein.	
GPO-Computer-Sicherheit-Scope-Clients-WSITS		Einstellung Status	
GPO-Computer-Sicherheit-Scope-Server-HyperV	111	Software\Policies\Microsoft\Windows 1	
GPO-Computer-Sicherheit-Scope-Server-JB     GPO-Computer-Sicherheit-Scope-Server-JB	111	Defender\MpEngine \MpEnablePus	
GPO-Computer-Sicherheit-Scope-Server-Monitorin     GPO-Computer-Sicherheit-Scope-Server-Monitorin			
GPO-Computer-Sicherheit-Scope-Server-MX     GPO-Computer-Sicherheit Server Spece BDS	Ber	nutzerkonfiguration (Deaktiviert)	Auchine day
GPO-Computer-Sicherheit-Scope-Server-RDS     GPO-Computer-Sicherheit-Scope-Server-RDS		Keina Finstellunnan definiert	Ausbienden
CPO Computer-Sicherheit-Scope-Server-Standard		None Enacolonger dennier	

#### Vergleich zwischen zwei GPO mit dem PolicyAnalyzer (SCT)

VS IT-Solutions

Einen Sonderfall möchte ich hier aufzeigen. Ich verwende eine alte GPO für die Härtung des Internet Explorers. Diese GPO hat ihren Ursprung ebenfalls in einer Microsoft-Security-Baseline-GPO aus dem Security Compliance Toolkit. Im aktuellen Paket des SCT ist auch eine Version mit dabei. Da der Internet Explorer auch auf anderen Betriebssystemen in der Version 11 vorhanden ist, stehe ich nun vor folgender Frage: "Hat sich etwas zwischen den beiden GPO-Versionen verändert?" Wenn sich nichts verändert hat, dann kann ich die neue Version auch ungeprüft auf die bestehenden Systeme anwenden. Wurden aber Veränderungen vorgenommen, dann muss ich einen Test der GPO durchführen.

Solche Testphasen können sehr zeitintensiv sein. Schneller geht daher ein Vergleich der beiden GPO. Leider sind hier unzählige Einstellungen in beiden Versionen vorhanden. Eine manuelle Sichtung ist nicht möglich! Den Vergleich kann ich aber mit dem kostenlosen PolicyAnalyzer von Microsoft vornehmen. Der gehört zum SCT dazu.

Zuerst exportiere ich meine aktive GPO durch eine Sicherung:

Microsoft Exchange Security Groups	^	ws							
🤉 🔤 wa		Verknüpft	e Gruppenrichtlinienobje	ekte Grupper	nrichtlinienvererbung Delegierun	g			
Ordpperintentimenobjekte     Option     Option			Verknünfungereih	enfolce	Gruppenrichtlinienshiekt	Framingen	Verknünfung aktiviert	Objektetatue	WM
Default Domain Controllers Policy     Pefault Domain Policy			verknuprungsrein	enioige	Citopperinci i interiobjekt	Lizwungen	verki uprung aktivien	Objektstatus	4414
GPO-Beputzer									
GPO-Benutzer-Ordnerumleitung									
GPO-Benutzer-BDS									
GPO-Benutzer-Sicherheit-Office-20	)16								
GPO-Benutzer-Zertifikate									
GPO-Clients-RDS									
GPO-Clients-Win10-1803-Datensch	utz								
GPO-Clients-Win10-1803-Konfigur	ation								
GPO-Clients-Win10-1803-Sicherhei	it								
GPO-Clients-Win10-1903-Datensch	utz								
GPO-Clients-Win10-1903-Konfigur	ation								
GPO-Clients-Win10-1903-Konfigur	ation-PineAP								
GPO-Clients-Win10-1903-Sicherhei	it								
GPO-Clients-Win10-1909-Dater	Bearbeiten								
GPO-Clients-Win10-1909-Konfi	Obiektstatus		>						
GPO-Clients-Win10-1909-Siche									
GPO-Computer-Benutzerprofile	Sichern								
GPO-Computer-MSRA	Von Sicherung w	iederherstel	len						
GPO-Computer-Sicherheit-App	Einstellungen im	portieren							
GPO-Computer-Sicherheit-Aud	Baricht spaichore								
GPO-Computer-Sicherheit-Aud	bencht speichen								
GPO-Computer-Sicherheit-Basi	Neues Fenster hi	er öffnen							
GPO-Computer-Sicherheit-Bitle									
GPO-Computer-Sicherheit-Cipł	Kopieren								
GPO-Computer-Sicherheit-DC	Löschen								
GPO-Computer-Sicherheit-Defe	Umbenennen								
GPO-Computer-Sicherheit-Dev	Aktualisieren								
GPO-Computer-Sicherheit-Firet									
GPO-Computer-Sicherheit-Fire	Hilfe								



Jetzt starte ich den PolicyAnalyzer:

WS IT-Solutions

ei Start Freigeben Ansicht	Anwendungstools				
Ansient Ansient	Zwirchenshlage + SCT + DeligeApplager +		"Rolig:Apphage" durd	hrushan	
	Zwischenablage / SCT / PolicyAnalyzer /	V 0 /	PolicyAnalyzer durch	nsuchen	
Dieser PC	Name	Änderungsdatum	Тур	Größe	
🧊 3D-Objekte	PolicyRules	14.07.2019 12:24	Dateiordner		
📰 Bilder	SamplePolicyRules	30.12.2019 11:45	Dateiordner		
Desktop	Merge-PolicyRules.ps1	03.10.2016 22:33	Windows PowerS	1 KB	
🔁 Dokumente	policy Analyzer.pdf	01.06.2017 18:44	PDF-Datei	1.249 KB	
🕹 Downloads	PolicyAnalyzer.exe	27.06.2018 16:34	Anwendung	240 KB	
h Musik	PolicyAnalyzer_GetLocalPolicy.exe	27.06.2018 16:34	Anwendung	28 KB	
Videos	PolicyRulesFileBuilder.exe	27.06.2018 16:34	Anwendung	306 KB	
Lokaler Datenträger (C:)	Split-PolicyRules.ps1	01.06.2017 18:24	Windows PowerS	2 KB	
M DVD-Laufwerk (D:) CPBA_X64FR					
🛖 Freigaben (M:)					
Zwischenablage					
ADMX					
SCT					
Baselines					
-					

Im Menü kann ich nun die GPOs importieren:



Dicy Analyzer v3.2.1803.28001	– 🗆 X
Select All Compare local registry Local policy 👻 0 selected	
Name Date Size	Add
Policy File Importer X	
File     Edit       Add files from GPO(s)     Add Computer Configuration (registry.pol)	View / Compare
Add User Configuration (registry.pol) Add Security Template (*.inf) Add Audit Policy (audit.csv)	Delete selected
Close	
Import	
Policy Rule sets in: C:\Users\admin-setup	
Policy Definitions in: C:\Windows\PolicyDefinitions	

Ich beginne mit der aktuellen Microsoft-Baseline. Im Hauptverzeichnis aus dem ZIP-Archiv finde ich die Ordner mit den Unique-ID-Bezeichnern. Es genügt, wenn der Ordner geöffnet wird:

	🗵 Policy Ana	lyzer v3.2.1803.28001					
	Select All	Compare local registry	📃 Local policy 🁻	0 selected	I.		
Windows 10 Version 1909 and Window	Name		Date	Size			
"e		P	Policy File Importer				- 0
Microsoft Edge		1	Browse for the root fold	er under wh	ich the GPO(s) are stored.		
		<b>f</b>		0 Version 190	9 and Windows Server Version 1909 Secu	urity Baseline\GPOs 🗠 🗸	O D G
			Organisieren 👻 🛛 Neu	er Ordner			
Windows 10 Version			Dieser PC	Name	^	Änderungsdatum	Тур
isos and window.			🧊 3D-Objekte	{4E6	0D2FB-5E65-4AAB-843E-836833DEFA	29.12.2019 15:33	Dateiordner
			📰 Bilder	6E2	073CE-B1B5-4A0F-B1E4-C007BD052B	29.12.2019 15:33	Dateiordner
			Desktop	{450	CA52BB-19DE-487A-9CE8-0A95B18F6	29.12.2019 15:33	Dateiordner
48681125-0661-4			{48C8E12E-06	{159	ECA05-4C14-4DE4-94FE-578543473D	29.12.2019 15:33	Dateiordner
			Windows 10 \	{365	7C7A2-3FF3-4C21-9439-8FDF549F1D	29.12.2019 15:33	Dateiordner
			Documenta	635	i9FA45-B4E8-4B56-864A-591B4DD864	29.12.2019 15:33	Dateiordner
			CD Decementa	{645	i8B19A-73D5-4F93-8841-DA93A72F18	29.12.2019 15:33	Dateiordner
			op Reports	AB	C66265-8884-49F9-9621-0213E3566A6	29.12.2019 15:33	Dateiordner
			GPOs Y	(DA	SAFEDE DAEC ATEL DEDU CELLTADEC	20 12 2010 15:22	Desclaration
			GPO	root folder:			
		L					Ordner auswäh
	Paliau Pula astr						
	Folicy hule set	sin. C. Osers admin-setup					
	Policy Definition	ns in: C:\Windows\PolicyDef	initions				

Der PolicyAnalyzer erkennt in den Unterverzeichnissen automatisch die GPOs. Hier finde ich die neue IE-Policy:



Select All Compare local	egistry 🗌 Local policy 👻 0 select	d				
Name	Date Si.					Add
	Policy File Importer File Edit			- 0	×	/iew / mpare
	Policy Name Policy Name MSFT Windows 10 1909 - BitLocker MSFT Windows Server 1909 - Member S MSFT Windows Server 1909 - Member S MSFT Windows 10 1909 - User MSFT Windows 10 1909 and Server 19() MSFT Windows Server 1909 - Domain C MSFT Windows 10 1909 and Server 19() MSFT Windows 10 1909 - Computer	Policy Type Computer ver Computer ver User User - Defender Antivirus Computer troller Computer troller Computer troller Computer troller Computer troller Computer troller Computer Computer Computer Computer Computer Computer Computer Computer	File name registry pol registry pol	Folder C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt C:\Users\admin-setup\Deskt	>           >	lected
Policy Rule sets in: C:\Users\admin	setup	Import			>	

Der PolicyAnalyzer konvertiert die GPO in eine PolicyRule-Datei. Diese muss wieder gespeichert werden:

ame	Date Size		Add
	D Policy File Importer		× /iew /
	🔎 Save imported Policy Rules		
	← → · ↑	1909 and Windows Server Vers > v	C "Windows 10 Version 19
	Organisieren 👻 Neuer Ordner		
	3D-Objekte ^ Name ^	Änderungsdatum	Typ Größe
	Bilder Documentation	29.12.2019 15:33	Dateiordner
	Desktop GP Reports	29.12.2019 15:33	Dateiordner
	48C8E12E-06 GPOs	29.12.2019 15:33	Dateiordner
	Windows 10 \	29.12.2019 15:33	Dateiordner
	Dokumente	29.12.2019 15:33	Dateiordner
	Jownloads V		
	Datei <u>n</u> ame: IE-Baseline-1909		
	Dateityp: Policy Rules (*.PolicyRules)		
			Speichern Abbrec
	<ul> <li>Ordner ausbienden</li> </ul>		2perchem Abbrech

Jetzt kommt meine aktive GPO dran. Der Import-Assistent funktioniert genauso:

## WS IT-Solutions

## WSHowTo – moderne GPO-Versionierung am Beispiel Windows 10 2020-01-30 Gruppenrichtlinien

🔎 Policy An	alyzer v3.2.1803.28001	- 🗆 ×
Select All	Compare local registry Local policy 👻 0 selected	
Select All	Compare local registry     Local policy      O selected      Date     Size  Policy File Importer     -	Add,         View /         Compare         Delete         selected
D Policy An	alyzer v3.2.1803.28001	– 🗆 X

Policy File Importer	Date	Size		- 🗆 🗙		Add
🗵 Browse for the root folde	r under which the GPO(s) are	stored.			×	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ > Di	eser PC > Desktop >		~ (	ے پاک	" durchsuchen	View
Organisieren 🔻 Neue	Ordner				::: - ?	Compa
	Name (48C8E12E-06C1-4DF/	Ā.         -9E90-A00DD7FF4         30           909 and Windows S         31	nderungsdatum .12.2019 11:47 .12.2019 12:42	Typ Dateiordner Dateiordner	Größe	Delete
GPO (	root folder: Desktop		Г	Ordner auswählen	Abbrechen	

ame 🗾 Policy Fi	le Importer	Llate	Size			- 0	×	Add
File Edit								
Policy Nam	e			Policy Type	File name	Folder	^	 View /
MSFT Wind	lows 10 1909 - Computer			Computer	registry.pol	C:\Users\admin-setup\Desktop	N	 Compar
GPO-Comp	uter-Sicherheit-IExplore			Computer	registry.pol	C:\Users\admin-setup\Desktop	N	 Compa
MSFT Wind	lows 10 1909 - BitLocker			Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	
MSFT Wind	lows Server 1909 - Member	r Server		Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	
MSFT Wind	lows 10 1909 and Server 1	909 - Domain Security		Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	 Delete
MSFT Inter	net Explorer 11 - Computer			Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	 selecte
MSFT Wind	dows Server 1909 - Domain	Controller		Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	
MSFT Wind	lows 10 1909 - Computer			Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop	N	
GPO-Comp	uter-Sicherheit-IExplore			Sec Template	GptTmpl.inf	C:\Users\admin-setup\Desktop		
MSFT Wind	lows Server 1909 - Member	r Server		Audit Policy	audit.csv	C:\Users\admin-setup\Desktop	N	
MSFT Wind	lows Server 1909 - Domain	Controller		Audit Policy	audit.csv	C:\Users\admin-setup\Desktop	N	
MSFT Wind	lows 10 1909 - Computer			Audit Policy	audit.csv	C:\Users\admin-setup\Desktop		
							*	

Und der Prozess wird mit der Erstellung der zweiten PolicyRule-Datei beendet:

ame 🗾 Poli	icy File Importer	Date Size		- 🗆 X	Add
🗵 Sa	ave imported Policy Rul	es			×
÷	→ • ↑ 📙 « Des	sk > Windows 10 Version 1909 and Windo	ows Server Vers > v	ල "Windows 10 Version	1909 a View /
Orga	anisieren 🔻 Neuer	Ordner		8== -	Compar
-	Dieser PC	Name	Änderungsdatum	Typ Größe	
	🗊 3D-Objekte	Documentation	29.12.2019 15:33	Dateiordner	Delete
	Nilder	GP Reports	29.12.2019 15:33	Dateiordner	Selecte
_	Desktop	GPOs	29.12.2019 15:33	Dateiordner	
	48C8E12E-06	Scripts	29.12.2019 15:33	Dateiordner	
	Windows 10 \		29.12.2019 15:33	Dateiordner	
	🗄 Dokumente 🗸	IE-Baseline-1909.PolicyRules	31.12.2019 12:42	POLICYRULES-Datei 295 K	(B
	Datei <u>n</u> ame: IE-GP	o			~
	Dateitura Bolica	Puler (* Policy/Puler)			

Jetzt stelle ich den Suchpfad um. Dazu muss auf den Schalter im unteren Bereich geklickt werden:

WS IT-Solutions

🗾 Policy Analy	yzer v3.2.1803.28001				– 🗆 X
Select All	Compare local registry	📃 Local policy 👻	0 selected		
Name		Date	Size		Add
					View /
					Compare
					Delete selected
Policy Rule sets	in: C:\Users\admin-setup				
Policy Definition:	s in: C:\Windows\PolicyDefi	nitions	- Click	to change Policy Rules folder	

Policy Analyzer v3.2.1803.2	8001				- 🗆 X
Pick the folder containing	g the Policy Analyzer Policy Rules files			×	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ $\rightarrow$ Win	ndows 10 Version 1909 and Windows Se	rver Version 1909 Secu 🗸 🗸	ර / "Win	dows 10 Version 1909 a	Add
Organisieren 🔻 Neuer	Ordner			≣≕ ▾ 😮	
👌 Musik \land	Name	Änderungsdatum	Тур	Größe	View
Videos	Documentation	29.12.2019 15:33	Dateiordner		Compare
🏪 Lokaler Datentı	GP Reports	29.12.2019 15:33	Dateiordner		
🖆 DVD-Laufwerk	GPOs	29.12.2019 15:33	Dateiordner		
🛖 Freigaben (M:)	Scripts	29.12.2019 15:33	Dateiordner		Delete
青 Bibliotheken	Templates	29.12.2019 15:33	Dateiordner		selected
💣 Netzwerk					
48C8E12E-06C1					
Windows 10 Vers 🗡					
Folder	r containing PolicyRules files Windows	s 10 Version 1909 and Windows Serve	r Version 1909 Security	Baseline	
			Ordner auswähl	en Abbrechen	

Jetzt werden die beiden PolicyRule-Dateien angezeigt. Der Rest ist einfach: Für den direkten Vergleich wähle ich beide aus:

me	Date	Size	
E-Baseline-1909	31.12.2019 12:42:15	301.912	Add
IE-GPO	31.12.2019 12:44:41	354.015	
			View Compa
			Delete

Im Vergleichsfenster kann ich nun die Anzeige filtern und identische Einstellungen ausblenden:



🗵 Policy Viewer -	386 items				- 0	×
🗄 Clipboard 🗸 Viev	🗸 🗸 👬 - Export - Options -					
Policy Type	Show only Differences		Policy Setting	IE-Baseline-1909	IE-GPO	^
Audit Policy	Channes he Canellista		Andere Anmelde-/Abmeldeereignisse überwachen	Success and Failure	Success and Failure	
Audit Policy	Show only Conflicts		Anmelden überwachen	Success and Failure	Success and Failure	
Audit Policy 🗸	Show Details Pane		Kontosperrung überwachen	Failure	Failure	
Audit Policy	Show because and		Mitgliedschaft in der Überwachungsgruppe	Success	Success	
Audit Policy	GPO filter		Spezielle Anmeldung überwachen	Success	Success	
Audit Policy	Berechtigungen		Sensible Verwendung von Rechten überwachen	Success and Failure	Success and Failure	
Audit Policy	Detaillierte Überwachung		PNP-Überwachungsaktivität	Success	Success	
Audit Policy	Detaillierte Überwachung		Prozesserstellung überwachen	Success	Success	
Audit Policy	DS-Zugriff		Verzeichnisdienständerungen überwachen	Success	Success	
Audit Policy	DS-Zugriff		Verzeichnisdienstzugriff überwachen	Failure	Failure	
Audit Policy	Kontenverwaltung		Andere Kontoverwaltungsereignisse überwachen	Success	Success	
Audit Policy	Kontenverwaltung		Benutzerkontenverwaltung überwachen	Success and Failure	Success and Failure	
Audit Policy	Kontenverwaltung		Computerkontoverwaltung überwachen	Success	Success	
Audit Policy	Kontenverwaltung		Sicherheitsgruppenverwaltung überwachen	Success	Success	
Audit Policy	Kontoanmeldung		Kerberos-Authentifizierungsdienst überwachen	Success and Failure	Success and Failure	
Audit Policy	Kontoanmeldung		Ticketvorgänge des Kerberos-Diensts überwachen	Failure	Failure	
Audit Policy	Kontoanmeldung		Überprüfen der Anmeldeinformationen überwachen	***CONFLICT***	***CONFLICT***	
Audit Policy	Objektzugriff		Andere Objektzugriffsereignisse überwachen	Success and Failure	Success and Failure	
Policy Path: Advanced Audit Policy\DS-Zı. Verzeichnisdienstäi Objektänderung Mithilfe dieser F pi Falls möglich, g	slicy Configuration ggrff Inderungen überwachen gen der Active Directory Domain Se Richtlinieneinstellung können Sie Ei orokolliet, wen ein Ötjekt erstellt, eben die in dieser Unterkategorie p	rvices eignisse überwachen, die durch / gelöscht, geändert, verschoben rotokollierten Ereignisse die atten	Inderungen an den AD DS-Objekten (Active Directory Do oder wiederhergesteilt wird. und neuen Werte der Objekteigenschaften an.	nain Services) generiert wu	rden. Die Ereignisse werden	^
Die Ereignisse ( Li Hinweis: Die Ak	dieser Unterkategorie werden nur a ist, SACL) protokolliert. ktionen für einige Objekte und Eige	uf Domänencontrollem protokollie nschaften verursachen aufgrund	rt, und es werden nur Objekte in AD DS mit übereinstimme der Einstellungen für die Objektklasse im Schema keine G	nder Systemzugriff-Steuerui enerierung von Überwachui	ngsliste (System Access Control ngsereignissen.	
Wenn Sie diese	e Richtlinieneinstellunn konfinuriere	n wird heim Ändern eines Ohiekte	in AD DS ein Ühenvachungsphiekt generiet. Mithi			¥

Und aus unzähligen Einstellungen in beiden GPO sehe ich die wenigen Unterschiede. Diese kann ich nun einzeln prüfen und danach entscheiden, ob die GPO mit den neuen Einstellungen freigegeben werden kann:

🗵 Policy Viewer -	12 items			- 0	×
Clipboard - View	• 🙀 • Export • Options •				
Policy Type	Policy Group or Registry Key	Policy Setting	IE-Baseline-1909	IE-GPO	
Audit Policy	Kontoanmeldung	Überprüfen der Anmeldeinformationen überwachen	***CONFLICT***	***CONFLICT***	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	ListBox Support ZoneMapKey		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	UNCAsIntranet	0	***CONFLICT***	<u> </u>
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	file://ws.its		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	file://ws-fs1.ws.its		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	file://ws-fs2.ws.its		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	https://secure.comodo.com		2	
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceGuard	LsaCfgFlags	***CONFLICT***	***CONFLICT***	<u> </u>
Security Template	Privilege Rights	SeDenyNetworkLogonRight	***CONFLICT***	***CONFLICT***	_
Security Template	Privilege Rights	SeEnableDelegationPrivilege	***CONFLICT***	***CONFLICT***	_
Security Template	Privilege Rights	SeInteractiveLogonRight	***CONFLICT***	***CONFLICT***	_
Security Template	Privilege Rights	SeNetworkLogonRight	***CONFLICT***	***CONFLICT***	_
Policy Path					_
Advanced Audit Pol Audit Policy\Kontoa Überprüfen der Anm	icy Configuration nmeldung eldeinformationen überwachen				
Uberprüfung der	Anmeldeinformationen				
Mithilfe dieser Ri	chtlinieneinstellung können Sie Ereignisse überwachen, die durch Va	lidierungstests der Anmeldeinformationen für Benutzerkom	ten generiert wurden.		
Die Ereignisse in Ko	dieser Unterkategorie treten nur auf dem Computer auf, der für diese nten ist der lokale Computer autorisierend.	Anmeldeinformationen autorisierend ist. Bei Domänenkor	nten ist der Domänencontrol	ller autorisierend. Bei lokalen	
Volume: Hoch a Standardeinstell	uf Domänencontrollern. ung auf Clients: Keine Überwachung.				
Standardeinstell	ung auf Servern: Erfolg.				
IE-Rasolino-100	0-				~



🗾 Policy Vie	ewer - 12 items			_	×
Clipboard	• View • 🙀 • Export • Options •				
Policy Type	Policy Group or Registry Key	Policy Setting	IE-Baseline-1909	IE-GPO	^
Audit Policy	Kontoanmeldung	Überprüfen der Anmeldeinformationen überwachen	***CONFLICT***	***CONFLICT***	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	ListBox Support ZoneMapKey		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	UNCAsIntranet	0	***CONFLICT***	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	file://ws.its		1	
HKLM	Software\Policies\Microsoft\Windows\CurrentVersion\Internet S	file://ws-fs1.ws.its		1	
HKLM	Software \Policies \Microsoft \Windows \Current Version \Internet S	file://ws-fs2.ws.its		1	~
Intranetsites Diese Ri Wenn Si Wenn Si UE-Baselin- Option: Data: Type: GPO: IE-GPO: Option: Data: Type: GPO: Option: Data: Type: GPO: Option: Data: Type: GPO:	: Alle Netzwerkpfade (UNCs) einbeziehen ichtlinieneinstellung steuert, ob URLs, die für UNCs stehen, der Sicherheitszo ie diese Richtlinieneinstellung aktivieren, werden alle Netzwerkpfade der Intra ie diese Richtlinieneinstellung deaktivieren, werden Netzwerkpfade nicht not ie diese Richtlinieneinstellung nicht konfigurieren, werden die Benutzer gefrag <b>e-1909:</b> Disabled 0 REG_DWORD MSFT Internet Explorer 11 - Computer Disabled 0 0 0 0 0 0 0 0 0 0 0 0 0	ne des lokalen Intranets zugeordnet werden. anetzone zugeordnet. wendigenweise der Intranetzone zugeordnet (hier können d pt, ob Netzwerkpfade der Intranetzone zugeordnet werden	andere Regeln greifen).		

Das geht doch wesentlich schneller als ein vollständiger Testlauf, oder?

#### GPO anwenden

Meine neuen GPO sind fertig. Jetzt verknüpfe ich sie auf die gewünschten Organisationseinheiten. Natürlich sollten nur Testsysteme damit konfiguriert werden. Ggf. gibt es ja noch Anpassungsbedarf:

📓 Gruppenrichtlinienverwaltung								- 0	×
🔜 Datei Aktion Ansicht Fe	nster ?							-	8 ×
								]	
✓ ▲ Gesamtstruktur: ws.its	~	Gru	ppenrichtlinie	nobjekte in w	s.its				
🗸 📑 Domänen		Inha	lt Delegiening	•					
✓ iii ws.its			Delegierung						
🛒 Default Domain	Policy	Na	ame		Objektstatus	WMI-Filter	Geändert	Besitzer	^
> 📔 Domain Control	lers		Default Domain Cor	ntrollers Policy	Benutzerkonfigurationseins	Keine	27.10.2019 17:32:40	Domänen-Admins (W	
> 📔 Microsoft Excha	nge Security Groups		Default Domain Pol	icy	Benutzerkonfigurationseins	Keine	27.10.2019 17:32:38	Domänen-Admins (W	
🗸 📴 WS			GPO-Benutzer		Computerkonfigurationsein	Keine	27.10.2019 17:32:40	Domänen-Admins (W	
> 📄 AdminArea			GPO-Benutzer-Ordr	nerumleitung	Computerkonfigurationsein	Keine	27.10.2019 17:32:42	Domänen-Admins (W	
> 🚊 Benutzer			GPO-Benutzer-RDS	6	Computerkonfigurationsein	Keine	27.10.2019 17:32:38	Domänen-Admins (W	
✓ iii Clients			GPO-Benutzer-Sich	erheit-Office-2016	Computerkonfigurationsein	Keine	15.11.2019 18:55:54	admin-setup (admin-s	
ST GPC	Gruppenrichtlinienobjekt hier erstellen u	und verkr	nüpfen	ikate	Computerkonfigurationsein	Keine	27.10.2019 17:32:40	Domänen-Admins (W	
GPC	Vorbandenes Gruppenrichtlinienobiekt	/erknüpf	en		Benutzerkonfigurationseins	Keine	27.10.2019 17:32:42	Domänen-Admins (W	
GPC	Verenhumen elementériesen	_		1803-Datenschutz	Benutzerkonfigurationseins	Windows-10-1803	27.10.2019 17:32:42	Domänen-Admins (W	
GPC	vererbung deaktivieren			1803-Konfigurati	Benutzerkonfigurationseins	Windows-10-1803	27.10.2019 17:32:40	Domänen-Admins (W	
I GPC	Gruppenrichtlinienupdate			1803-Sicherheit	Benutzerkonfigurationseins	Windows-10-1803	27.10.2019 17:32:42	Domänen-Admins (W	
	Communicated in income delline and a size			1903-Datenschutz	Benutzerkonfigurationseins	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (W	
	Gruppenrichtlinienmodellierungs-Assist	ent		1903-Konfigurati	Benutzerkonfigurationseins	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (W	
	Neue Organisationseinheit			1903-Konfigurati	Benutzerkonfigurationseins	Windows-10-1903	27.10.2019 17:32:38	Domänen-Admins (W	
	Name Franks bin affrage			1903-Sicherheit	Benutzerkonfigurationseins	Windows-10-1903	27.10.2019 17:32:40	Domänen-Admins (W	
GPC	Neues renster hier offnen			1909-Datenschutz	Benutzerkonfigurationseins	Windows-10-1909	29.12.2019 17:09:12	Domänen-Admins (W	
GPC GPC	Löschen			1909-Konfigurati	Benutzerkonfigurationseins	Windows-10-1909	29.12.2019 15:22:44	Domänen-Admins (W	
GPC GPC	Aktualisioron			1909-Sicherheit	Benutzerkonfigurationseins	Windows-10-1909	29.12.2019 15:38:40	Domänen-Admins (W	
GPC	Aktualisieren			.tzerprofile	Benutzerkonfigurationseins	Keine	27.10.2019 17:32:42	Domänen-Admins (W	
GPC	Eigenschaften			RA .	Benutzerkonfigurationseins	Keine	27.10.2019 17:32:42	Domänen-Admins (W	
GPC				erheit-Applocker	Benutzerkonfigurationseins	Keine	27.10.2019 17:32:40	Domänen-Admins (W	
GPC	Hilfe			erheit-Audit	Benutzerkonfigurationseins	Keine	01.12.2019 16:54:18	Domänen-Admins (W	

📓 Gruppenrichtlinienverwaltung								×
📓 Datei Aktion Ansicht Fenster ?							-	ēΧ
♦ ♦ 2 m □ 0 0 0 m								
	^	Gruppenrichtlinienobjekte in Inhalt Delegierung	ws.its					
🛒 Default Domain Policy		Name	Objektstatus	WMI-F	iter	Geändert	Besitzer	^
> 🖬 Domain Controllers		Default Domain Controllers Policy	Benutzerkonfigurationseins	Keine		27.10.2019 17:32:40	Domänen-Admins (W	
> Microsoft Exchange Security Groups		Comparison Policy	Benutzerkonfigurationseins	Keine		27.10.2019 17:32:38	Domänen-Admins (W	
🗸 📴 WS	Grup	penrichtlinienobiekt auswählen		×		27.10.2019 17:32:40	Domänen-Admins (W	
> 📓 AdminArea		,				27.10.2019 17:32:42	Domänen-Admins (W	
> 📓 Benutzer	Für D	jomäne:				27.10.2019 17:32:38	Domänen-Admins (W	
✓ G Clients		the second second				15.11.2019 18:55:54	admin-setup (admin-s	
GPO-Clients-RDS		ws.its		~		27.10.2019 17:32:40	Domänen-Admins (W	
GPO-Clients-Win10-1803-Datenschutz	Grup	penrichtlinienobiekte:				27.10.2019 17:32:42	Domänen-Admins (W	
GPO-Clients-Win10-1803-Konfiguration					s-10-1803	27.10.2019 17:32:42	Domänen-Admins (W	
GPO-Clients-Win10-1803-Sicherheit		Name		^	s-10-1803	27.10.2019 17:32:40	Domänen-Admins (W	
GPO-Clients-Win10-1903-Datenschutz		GPO-Clients-Win10-1903-Konfiguration			s-10-1803	27.10.2019 17:32:42	Domanen-Admins (W	
GPO-Clients-Win10-1903-Konfiguration		GPO-Clients-Win10-1903-Konfiguration-Pi	neAP		s-10-1903	27.10.2019 17:32:38	Domanen-Admins (W	
GPO-Clients-Win10-1903-Sicherheit		GPO-Clients-Win 10-1903-Sicherheit			s-10-1903	27.10.2019 17:32:38	Domanen-Admins (W	
GPO-Computer-MSRA		GPO-Clients-Win10-1909-Datenschutz			s-10-1903	27.10.2019 17:32:38	Domanen-Admins (W	
GPO-Computer-Sicherheit-Applocker		GPO-Clients-Win10-1909-Konfiguration			s-10-1505	27.10.2013 17.32.40	Domanen-Admins (W	
GPO-Computer-Sicherheit-Audit		GPO-Clients-Win 10-1909-Sicherheit			s-10-1303	29.12.2019 17.09.12	Domanen-Admins (W	
GPO-Computer-Sicherheit-Basics		GPO-Computer-Benutzerprofile			e-10-1909	29 12 2019 15:38:40	Domänen-Admine (W	
GPO-Computer-Sicherheit-Bitlocker		GPO-Computer-MSRA			3-10-1303	27 10 2019 17:32:42	Domänen-Admine (W	
GPO-Computer-Sicherheit-Cipher-TLS		GPO-Computer-Sicherheit-Applocker				27 10 2019 17:32:42	Domänen-Admins (W	
GPO-Computer-Sicherheit-DeviceGuard		GPO-Computer-Sicherheit-Audit		~		27 10 2019 17:32:40	Domänen-Admins (W	
GPO-Computer-Sicherheit-Firefox						01.12.2019 16:54:18	Domänen-Admins (W	
GPO-Computer-Sicherheit-Firewall						27.10.2019 17:32:42	Domänen-Admins (W	
GPO-Computer-Sicherheit-IExplore						05.12.2019 17:45:24	Domänen-Admins (W	
GPO-Computer-Sicherheit-LAPS-Clients			OK Abbre	chen		27.10.2019 17:32:38	Domänen-Admins (W	
GPO-Computer-Sicherheit-I SAProtection						27.10.2019 17:32:42	Domänen-Admins (W	
		CDO Comertor Sicharhoit DC	Dani tradi anfini intianaaina	Kaina	_	07 10 0010 17-00-00	Dominon Admino (M	

Die Reihenfolge in der GPO-Verarbeitung spielt in meinem Schema eine wichtige Rolle. Die Richtlinien werden in der Reihenfolge von "unten" nach "oben" verarbeitet. Dabei überschreibt eine GPO mit einer kleineren Rangfolge die Einstellungen der GPO mit größerer Rangfolge. Die Reihenfolge meiner GPO muss zwingend so aussehen:

Zuerst wird die unmodifizierte Sicherheits-GPO angwendet.

WS IT-Solutions

- Deren Einstellungen werden von der Datenschutz-GPO ergänzt und überlagert (Sicherheit vs. Datenschutz...).
- Da auch die Datenschutz-GPO von externen Quellen stammen kann, würde ich auch deren Einstellungen mit der Konfigurations-GPO korrigieren. Daher kommt diese GPO an der dritten Stelle. Dadurch wird auch die Sicherheits-GPO überlagert.

Durch das freie Verbinden der GPOs auf die Organisationseinheit passt die Reihenfolge nicht:



Mit wenigen Klicks kann die Reihenfolge aber leicht angepasst werden. So ist es fein:

K Gruppenrichtlinienverwaltung								- 1		×
📓 Datei Aktion Ansicht Fenster ?									- 6	s ×
(= -) ( <u>2</u>										_
✓ A Gesamtstruktur: ws.its	^	Client	۰ <u>د</u>							
V 📓 Domänen		Vadrai	infta Grunnanrichtlinianshiakta	Compared bills to see the set of the second						
✓ jiii ws.its		VEININ	pre oropper norminer topjekte	Gruppenrichtlinienvereibung Deiegierung						
📓 Default Domain Policy			Verknüpfungsreihenfolge	Gruppenrichtlinienobjekt	Erzwungen	Verknü	Objektstatus	WMI-Filter		G
> Domain Controllers		$\Rightarrow$	1	GPO-Clients-RDS	Nein	Nein	Benutzerkonfig	Keine		2
> Dicrosoft Exchange Security Groups			2	GPO-Computer-MSRA	Nein	Ja	Benutzerkonfig	Keine		2
🗸 📴 WS			3	GPO-Computer-Sicherheit-UAC-light	Nein	Ja	Benutzerkonfig	Keine		2
> 🗾 AdminArea		$\nabla$	4	GPO-Computer-Sicherheit-Applocker	Nein	Ja	Benutzerkonfig	Keine		2
> 📓 Benutzer			5	GPO-Computer-Sicherheit-DeviceGuard	Nein	Ja	Benutzerkonfig	Keine		2
✓ iii Clients			6	GPO-Computer-Sicherheit-LSAProtection	Nein	Ja	Benutzerkonfig	Keine		0
GPO-Clients-RDS			7	GPO-Computer-Sicherheit-Firewall	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1803-Datenschutz			8	GPO-Computer-Sicherheit-Cipher-TLS	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1803-Konfiguration			9	GPO-Computer-Sicherheit-Basics	Nein	Ja	Benutzerkonfig	Keine		0
GPO-Clients-Win10-1803-Sicherheit			10	GPO-Computer-Sicherheit-LAPS-Clients	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1903-Datenschutz			11	GPO-Computer-Sicherheit-Netzwerk	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1903-Konfiguration			12	GPO-Computer-Sicherheit-Bitlocker	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1903-Sicherheit			13	GPO-Computer-Sicherheit-Zertifikate	Nein	Ja	Benutzerkonfig	Keine		2
GPO_Clients-Win10-1909-Datenschutz			14	GPO-Computer-Sicherheit-SmartCard	Nein	Nein	Benutzerkonfig	Keine		2
GPO-Clients-Win10-1909-Konfiguration			15	GPO-Computer-Sicherheit-Audit	Nein	Ja	Benutzerkonfig	Keine		0
GPO-Clients-Win10-1909-Sicherheit			16	GPO-Computer-Sicherheit-PowerShellWi	Nein	Ja	Benutzerkonfig	Keine		2
GPO Computer MSPA			17	GPO-Computer-Sicherheit-IExplore	Nein	Ja	Benutzerkonfig	Keine		2
CPO Computer-Misica			18	GPO-Computer-Sicherheit-Firefox	Nein	Ja	Benutzerkonfig	Keine		2
GPO-Computer-Sicherheit-Applocker			19	GPO-Clients-Win10-1803-Konfiguration	Nein	Ja	Benutzerkonfig	Windows-10-	1803	2
GPO-Computer-Sicherheit-Audit			20	GPO-Clients-Win10-1803-Datenschutz	Nein	Ja	Benutzerkonfig	Windows-10-	1803	2
GPO-Computer-Sicherheit-Basics			21	GPO-Clients-Win10-1803-Sicherheit	Nein	Ja	Benutzerkonfig	Windows-10-	1803	2
GPO-Computer-Sicherheit-Bitlocker			22	GPO-Clients-Win10-1903-Konfiguration	Nein	Ja	Benutzerkonfig	Windows-10-	1903	2
GPO-Computer-Sicherheit-Cipher-TLS			23	GPO-Clients-Win 10-1903-Datenschutz	Nein	Ja	Benutzerkonfig	Windows-10-	1903	2
GPO-Computer-Sicherheit-DeviceGuard			24	I GPO-Clients-Win 10-1903-Sicherheit	ivein	Ja	Benutzerkonfig	vvindows-10-	1903	2
GPO-Computer-Sicherheit-Firefox			25	B GPO-Clients-Win 10-1909-Konfiguration	ivein	Ja	Benutzerkonfig	windows-10-	1909	4
GPO-Computer-Sicherheit-Firewall			26	GPO-Clients-Win 10-1909-Datenschutz	Nein	Ja	Benutzerkonfig	Windows-10-	1909	2
GPO-Computer-Sicherheit-IExplore			27	BPO-Clients-Win 10-1909-Sicherheit	Nein	Ja	Benutzerkonfig	Windows-10-	1909	2

#### <u>Testlauf</u>

Normalerweise würde ich noch einen Sicherheitsfilter auf eine Testgruppe von Computern einrichten, bevor ich die GPOs verknüpfe. In meinem Fall gibt es aber nur den Editor-PC und einen bereits produktiven Client mit Windows 10 Version 1909. Alle anderen Clients arbeiten noch mit 1903. Das ist Einschränkung genug.

Dennoch teste ich die Richtlinien mit meinem Editor-Rechner. In größeren Umgebungen würde ich dafür separate Computer verwenden. Falls ich mich durch die GPOs aussperre, komme ich sonst vielleicht nicht mehr an die Konfigurationsoberfläche heran. Und nicht jede GPO-Einstellung wird wirkungslos, wenn man den Link der GPO entfernt.

Ich aktualisiere die Richtlinien des Computers:



Anschließend erstelle ich einen Gruppenrichtlinien-Bericht. Die neuen GPO werden als angewendet gelistet:



2 Administrator: Windows PowerShell —	×	
PS C:\Admin> PS C:\Admin> gpresult /H gpo.htm PS C:\Admin> .\gpo.htm PS C:\Admin>	Î	
E ← WS\admin-setup auf W × + ∨		- 🗆 ×
$\leftarrow$ $\rightarrow$ O $\widehat{\mathbf{a}}$ $\odot$  file:///C:/Admin/gpo.htm	□ ☆	¢ ℓ &
Gruppenrichtlinienergebnisse		
WS\admin-setup auf WS\WS-CL6 Dates emittelt an: 31 12 2019 12:57:16		Alle einblenden
Zusammenfassung		Ausblenden
Während der letzten Computerrichtlinie Aktualisierung am 31.12.2019 12:56:06		Addition
Keine Fehler entdeckt.		
Eine schnelle Verbindung wurde entdeckt. Weitere Informationen		
Während der letzten Gruppenrichtlinie Aktualisierung am 31.12.2019 12:52:02		
Keine Fehler entdeckt.		
Eine schnelle Verbindung wurde entdeckt. Weitere Informationen		
Computerdetails		Ausblenden
Allgemein		Einblenden
Komponentenstatus		Einblenden
Einstellungen		Einblenden
Gruppenrichtlinienobjekte		Ausblenden
Angewendete Gruppenrichtlinienobjekte		Ausblenden
Default Domain Policy [[31B2F340-016D-11D2-945F-00C04FB984F9]]		Einblenden
GPO-Clients-Win10-1909-Datenschutz [{6EA749F3-0605-4ABF-BECE-8E77546A2725}]		Einblenden
GPO-Clients-Win10-1909-Konfiguration {{9C6AC48E-ED4C-450B-BE2C-585EEE35E81C}}		Einblenden
GPO-Clients-Win10-1909-Sicherheit [{0899F345-0767-425C-9483-32898407F181}]		Einblenden
GPO-Computer-MSRA [[A12FB9D5-5486-4458-806A-7A59B9DE0C95]]		

Jede GPO transportiert Einstellungen, die von lokalen Hilfsprogrammen – den Client Side Extensions (im deutschen Client "Komponente" genannt) verstanden und verarbeitet werden. Auch diese sind alle erfolgreich durchgelaufen: Die erste Verarbeitung hat einige Sekunden in Anspruch genommen. Insgesamt wurden 12 Sekunden benötigt. Das ist noch in Ordnung:



Weitere Details finde ich in der Ereignisanzeige. Die Gruppenrichtlinien haben ein eigenes Eventlog:



Die Einträge liegen zeitlich dicht beieinander. Dennoch kann ich den Beginn der Gruppenrichtlinienverarbeitung leicht finden. Ab hier prüfe ich die Events von unten nach oben:

🛃 Ereignisa	nzeige						- 🗆	$\times$
Datei Aktio	on Ansicht ?							
(= =) 🆄								
			<b>F</b> · · · <b>F</b> • • • • • • • • • • • • • • • • • • •					_
>	EileHistory-Core A	Betriebsbereit Anzahl v	on Ereignissen: 5.011					
	FMS	Ebene	Datum und Uhrzeit	Q	)uelle	Ereignis-ID	Aufgabenkategorie	^
Ś	Folder Redirection	(i) Informationen	31.12.2019 12:55:48	G	roupPolicy (Micros	4017	Keine	
Ś	GenericRoaming	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	5320	Keine	
>	i glcnd	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	4326	Keine	
~	GroupPolicy	(i) Informationen	31.12.2019 12:55:47	G G	roupPolicy (Micros	5320	Keine	
	Betriebsbereit	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	5017	Keine	
>	HelloForBusiness	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	4017	Keine	
>	🗎 Help	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	5320	Keine	
>	HomeGroup Control P	(i) Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	5340	Keine	
>	HomeGroup Provider S	Informationen	31.12.2019 12:55:47	G	roupPolicy (Micros	4004	Keine	
>	HomeGroup-ListenerS	(i) Informationen	31.12.2019 12:52:02	G	roupPolicy (Micros	5117	Keine	
>	HotspotAuth	<ol> <li>Informationen</li> </ol>	31.12.2019 12:52:02	G	roupPolicy (Micros	8001	Keine	
~	HttpLog	<ol> <li>Informationen</li> </ol>	31.12.2019 12:52:02	G	roupPolicy (Micros	5016	Keine	
	Hupservice	(i) Informationen	31.12.2019 12:52:00	G	roupPolicy (Micros	4016	Keine	
(	Hvper-V-Hvpervisor	<ol> <li>Informationen</li> </ol>	31.12.2019 12:52:00	G	roupPolicy (Micros	5016	Keine	
Ś	Hvper-V-VID	<ol> <li>Informationen</li> </ol>	31.12.2019 12:51:58	G	roupPolicy (Micros	4016	Keine	
, ,	IdCtrls	<ol> <li>Informationen</li> </ol>	31.12.2019 12:51:58	G	roupPolicy (Micros	5016	Keine	~
>	International		ar awar a b	P 5				
>	International-Regional	Ereignis 4004, GroupPolicy	(Microsoft-Windows-GroupP	olicy)				*
>	Iphlpsvc	Allgemein Details						
>	IPxlatCfg							
>	KdsSvc	Die manuelle Verarbeit	ung der Richtlinie für Comput	er WS\WS-CL6\$ wird	gestartet.			-
>	Kernel-ApphelpCache	Aktivitäts-ID: {aad1fc7f	-3f6a-4c96-b94a-a93ebba67ab	51}				
>	Kernel-Boot							
>	Kernel-Event Iracing							
>	Kernel-IO							
>	Kernel-PhP	Protokollname:	Microsoft-Windows-GroupP	olicy/Betriebsbereit				
	Kernel-ShimEngine	Quelle:	GroupPolicy (Microsoft-Win	Protokolliert:	31.12.2019 12:55:47			
	Kernel-StoreMar	Ereignis-ID:	4004	Aufgabenkategorie:	Keine			
Ś	Kernel-WDI	Ehonor	Information on	Schlüssehuörten				
, ,	Kernel-WHEA	Ebene:	mornationen	schlusselworter:				
	Known Folders	Benutzer:	SYSTEM	Computer:	WS-CL6.ws.its			
>	LanguagePackSetup	Vorgangscode:	(1)					
>	LinkLayerDiscoveryPro	Weitere Informationen:	Onlinehilfe					
\	Liveld							

Auch hier wird bestätigt, welche Gruppenrichtlinien gefunden wurden:

WS IT-Solutions

WS IT-Solutions

## WSHowTo – moderne GPO-Versionierung am Beispiel Windows 10 2020-01-30 Gruppenrichtlinien

🛃 Ereignisanzeige					- 0	×
Datei Aktion Ansicht ?						
🗢 🔿 🖄 📷 🛛 🖬						
> FileHistory-Core	Betriebsbereit Anzahl	von Ereignissen: 5.011				
FileHistory-Engine FMS	Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie	^
> 📔 Folder Redirection	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5313	Keine	
> 🧮 GenericRoaming	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5312	Keine	
> 🛄 glcnd	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5126	Keine	
✓ GroupPolicy	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5216	Keine	
Betriebsbereit	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:49	GroupPolicy (Micros	4216	Keine	
> 🧮 HelloForBusiness	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:49	GroupPolicy (Micros	5257	Keine	
> 🧮 Help		21 12 2010 12 15 40	C D F 46	5017	W -	~
> HomeGroup Control P.	Ereignis 5312, GroupPolio	y (Microsoft-Windows-GroupPolicy)				×
> 🧾 HomeGroup Provider S	Alleensie D. 1					
> HomeGroup-ListenerS	Angemein Details					
> HotspotAuth	Lists day any used have	n Gruppensishtlinianahialatar				
> HttpLog	Liste der anwendbare	in Gruppennentimenobjekte:			^	
> HttpService	Default Domain Polic	y				
Hyper-V-Guest-Drivers	GPO-Clients-Win10-	1909-Sicherheit				
> Hyper-V-Hypervisor	GPO-Clients-Win10-	1909-Datenschutz				
JdCtde	GPO-Computer-Sich	erheit-Firefox				
> International	GPO-Computer-Sich	erheit-IExplore				
International-Regional	GPO-Computer-Sich	erheit-PowerShellWinRM				
	GPO-Computer-Sich	erheit-Audit				
IPxlatCfg	GPO-Computer-Sich	erneit-Zertifikate erheit-Bitlocker				
KdsSvc	GPO-Computer-Sich	erheit-Netzwerk				
> 🔛 Kernel-ApphelpCache	GPO-Computer-Sich	erheit-LAPS-Clients				
> 🔛 Kernel-Boot	GPO-Computer-Sich	erheit-Basics				
> 🧮 Kernel-EventTracing	GPO-Computer-Sich	erneit-Cipner-ILS erheit-Firewall				
> 🧮 Kernel-IO					•	

Ebenso zeigt das Eventlog, welche Richtlinien ausgelassen wurden. Natürlich mit Begründung:

🛃 Ereignisanzeige					- 0	×
Datei Aktion Ansicht ?						
🗢 🔿 🗾 🖬						
> FileHistory-Core	Betriebsbereit Anzah	von Ereignissen: 5.011				
> FileHistory-Engine	Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie	^
> Folder Redirection	(i) Informationen	31.12.2019 12:55:50	GroupPolicy (Micros	5320	Keine	
> 🧮 GenericRoaming	(i) Informationen	31.12.2019 12:55:50	GroupPolicy (Micros	5320	Keine	
> 🚞 glcnd	Informationen	31.12.2019 12:55:50	GroupPolicy (Micros	5313	Keine	
✓	(i) Informationen	31.12.2019 12:55:50	GroupPolicy (Micros	5312	Keine	
Betriebsbereit	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5126	Keine	
> 🧮 HelloForBusiness	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:50	GroupPolicy (Micros	5216	Keine	
> 🦰 Help		21.12.2010.12.55.40	C DF AF	4010	N .	
> 📔 HomeGroup Control P	Ereignis 5313, GroupPoli	cy (Microsoft-Windows-GroupPolicy)				×
> 🔛 HomeGroup Provider S	Allgomoin D-t-it-					
> HomeGroup-ListenerS	Aligemein Details					
> HotspotAuth	Dis Calana das Casas	- Aller - Marine - Aller - All	det de la transferie			
> HttpLog	Die folgenden Grupp	enrichtliniehobjekte wurden nicht ange	ewendet, da sie herausgeflitert wurden:		^	
> HttpService	Richtlinien der lokale	n Gruppe				
Hyper-V-Guest-Drivers	Nicht ange	vendet (Leer)				
> Hyper-V-Hypervisor	GPO-Clients-Win10-	1903-Konfiguration-PineAP				
> Hyper-v-vid	GPO-Computer-Sick	Sicherheit) erheit-UAC-light				
> dctris	Verweigert	(Sicherheit)				
> International-Regional	GPO-Clients-Win10-	1803-Konfiguration				
	Verweigert	(WMI-Filter)				
> Principate	Verweigert	1805-Datenschutz WMI-Filter)				
> KdsSvc	GPO-Clients-Win10-	1803-Sicherheit				
S Kernel-ApphelpCache	Verweigert	(WMI-Filter)				
Kernel-Root	GPO-Clients-Win10-	1903-Konfiguration				

Und hier wird aufgezeigt, welche Richtlinien verändert wurden:

WS IT-Solutions

🛃 Ereignisanzeige					- 0	×
Datei Aktion Ansicht ?						
🗢 🔿 🙍 💽 🚺						
> 📫 FileHistory-Core 🔺	Betriebsbereit Anzahl	von Ereignissen: 5.011				
> FileHistory-Engine	Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie	^
> 📔 Folder Redirection	Informationen	31.12.2019 12:55:54	GroupPolicy (Micros	4016	Keine	
> 🧮 GenericRoaming	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:54	GroupPolicy (Micros	5016	Keine	
> 📔 glcnd	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:54	GroupPolicy (Micros	4016	Keine	
✓	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:54	GroupPolicy (Micros	5016	Keine	
Betriebsbereit	<ol> <li>Informationen</li> </ol>	31.12.2019 12:55:54	GroupPolicy (Micros	4016	Keine	
> 📔 HelloForBusiness	(i) Informationen	31.12.2019 12:55:54	GroupPolicy (Micros	5016	Keine	
> 🧮 Help	ALC IS	21 12 2010 12 55 50	C BF AK	4010	N .	*
> HomeGroup Control P.	Ereignis 4016, GroupPolic	y (Microsoft-Windows-GroupPolicy)				×
> HomeGroup Provider S	Allgemein Deteile					
> HomeGroup-ListenerS	Angement Details					
> HotspotAuth	Die Verscheitung des f	Construction Construction and an advantage				e e e e e e e e e e e e e e e e e e e
> HttpLog	Die verarbeitung der :	security-Erweiterung wird gestartet.				
> Httpservice	Liste der anwendbare	n Gruppenrichtlinienobjekte: (Änderun	gen wurden ermittelt.)			
> Hyper-V-Guest-Drivers						
> Hyper-V-Hypervisor	Default Domain Polic	/ 000 Sinhashait				
> idCtds	GPO-Clients-Win10-1	909-Sichement 909-Konfiguration				
> International	GPO-Computer-Siche	rheit-PowerShellWinRM				
International-Begional	GPO-Computer-Siche	rheit-Audit				
	GPO-Computer-Siche	rheit-Basics				
> IPxlatCfg	GPO-Computer-Siche	rheit-Firewall				
> KdsSvc	GPO-Computer-Siche	rheit-Applocker				
> Kernel-ApphelpCache	GPO-Computer-Siche	rheit-Scope-Clients-WSITS				

Das scheint alles zu passen. Im nächsten Schritt starte ich den Client neu und prüfe anschließend die Eventlogs in der Zusammenfassung auf Warnungen und Fehler. Auch in den Details sind keine Probleme zu finden, deren Ursprung in den neuen Richtlinien liegt:



Weitere funktionale Tests sind natürlich auch notwendig. Ebenso wie die Überprüfung von Anwendungen. Dies kann üblicherweise an eine Pilotbenutzergruppe delegiert werden. Diese Personen erhalten das neue Betriebssystem und melden Probleme und Anpassungswünsche auf kurzen Wegen direkt zum GPO-Designer. In meinem Fall sind das meine lieben Kolleginnen in meinem Außenstandort.

Nachtrag: Auch nach mehreren Wochen gab es keine Probleme. Aus meiner Perspektive ist das neue Betriebssystem mit den Richtlinien wie gewohnt administrierbar. Einer Umstellung der anderen Clients auf Windows 10 Version 1909 steht nichts mehr im Wege.