ReDoKS 2.3

GPO-Detaildaten (Einstellungsinhalte) auswerten

Handbuch

Inhalt

1	Erm	itteln der Daten	3
	1.1	Vorgehensweise bei Export über die Gruppenrichtlinienverwaltung	3
	1.2	Vorgehensweise bei Export per PowerShell-Skript	4
2	Einle	esen und Auswerten der Daten	4
	2.1	Besonderheiten beim Vergleich von GPO-Inhalten	6

1 Ermitteln der Daten

Es können mit ReDokS Version 2.3 nun – anders als bisher – für GPOs auch Detaildaten über die in den Group Policys enthaltenen Einstellungen erfasst werden. Dazu müssen die entsprechenden Daten der GPOs zunächst exportiert werden. Dies kann entweder manuell über die Gruppenrichtlinienverwaltung oder über ein PowerShell-Skript erfolgen. Nach bisherigen Erkenntnissen ist die Ausführung des PowerShell-Skripts aber nur für die R-Domäne möglich (nicht aber für die IT-Cloud-Domäne). Falls jemand da einen Weg findet bin ich dankbar für eine Rückmeldung.

1.1 Vorgehensweise bei Export über die Gruppenrichtlinienverwaltung

- 1. Gruppenrichtlinienverwaltung öffnen
- 2. Ordner "Gruppenrichtlinienobjekte" auswählen
- 3. Gewünschte GPOs selektieren (Strg-A um alle zu selektieren)
- 4. Im Kontextmenü "Sichern..:" wählen
- 5. Als Zielverzeichnis das Unterverzeichnis "GPO" in dem Verzeichnis wählen, aus dem die *.domx-Datei im Viewer eingelesen wird

🗢 🔿 🙍 🗔 🛛 🖬			
Gruppenrichtlinienverwaltung ✓ A Gesamtstruktur: R2301.ads.fiducia.de ✓ A Domänen → R2201.ads.fiducia.da	Gruppenrichtlinienobjekte in Inhalt Delegierung	R2301.ads.fiducia.de	WALLES
 Resoltads.inducta.de Default Domain Policy DomPolicy2Enforced Admin-Root Domain Controllers Gruppenrichtlinienobjekte Starter-Gruppenrichtlinienobjekte Starter Standorte Gruppenrichtlinienmodellierung Gruppenrichtlinienergebnisse 	AdminRootPolicy AdminRootPolicy2 AdminRootPolicy3Cmp AdminRootPolicy4Deaktiviert AdminRootPolicy6Grp 1Denied Default Domain Controllers Policy Default Domain Policy DomPolicy1 DomPolicy2Enforced R0815_ReDoKS R2301_AdminVox_Copy R2301_AdminVox_Start R2301_Test UsrPolicy UsrPolicy2 VsrPolicy2	Objektstatus Aktiviert Aktiviert Aktiviert Alte Einstellungen deaktiviert Aktiviert Aktiviert	Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine Keine

So könnte die Verzeichnisstruktur dann aussehen:



1.2 Vorgehensweise bei Export per PowerShell-Skript

Der Export kann über das Powershell-Skript "get-gporeport" erzeugt werden:

Group Policy "MyGPO" exportieren:

get-gporeport -name "MyGPO" -reporttype xml -Path "X:\R0815\GPO\MyGPO.xml"

Alle Group Policies exportieren:

get-gporeport -all -reporttype xml -Path "X:\R0815\GPO\GPOs.xml"

Je nach Einsatzumfeld können auch noch zwei weitere Parameter sinnvoll sein:

-domaingibt die Domäne an, aus welcher GPOs exportiert werden sollen-servergibt den Domain Controller an, an den die Abfrage gerichtet wird

Die erzeugte(n) Datei(en) dann einfach in as Unterverzeichnis "GPO" in dem Verzeichnis ablegen, aus dem die *.domx-Datei im Viewer eingelesen wird

2 Einlesen und Auswerten der Daten

Im Ladedialog für die Domäne den Haken in der Spalte "GPO Daten" setzen:

🚰 Daten laden – 🗆 🗙											
Ladekonfiguration Manuell laden Sonstige Daten											
-v	Verzeichnisse										
Datenverzeichnis: F:\Data\ReDoKS\Scans											
1	Verzeichni	is mit PC-Daten (relativ zur *.o	domx-Datei):	PCs							
١	Verzeichni	is mit Vergleichs-PC-Daten (re	elativ zur *.domx-[Datei): PCs_alt							
: 6	Neu	🔯 Löschen							🛃 Speic	nern	
Ak Unterverzeichnis Dateimuster Unterverzeic Vergleichsdat GPO-Daten Jaden Server PC-Dat TraceLogon											
		bn-its	*				~			-	
►	\checkmark	r2301	*.domx		~						
		Test	*.domx				\checkmark	\checkmark			

Im Ladeverlauf kommen dann entsprechende Verarbeitungsmeldungen:

6	Cadeverlauf									
	Element	Dateiname	Beschreibung	Fehler						
	✓ ☐ 'r2301*.domx'									
	🗊 R2301	R2301_28-03-2022.domx	16 User, 60 Gruppen, 6 Computer							
000) =====================================				=		^			
000) Daten laden									
000) =====================================				=					
000	D Basisverzeichnis: F:\Data\]	ReDoKS\Scans			_					
000	Domänendaten laden aus 'r2'	301*_domx'			-					
000) -> 8 Dateien gefunden	ool (. doma								
000) Domänendatei laden: 'R2	301 28-03-2022.domx'								
000) ->geladen: 16 User,	60 Gruppen, 6 Computer								
000	GPO-Dateien laden									
000) 1/15: GPOs aus '{	22B0835F-09E8-4668-9D05-6AC85C7	DA105}\gpreport.xml' e	einlesen						
000) -> Daten zu 1 (GPOs eingelesen								
000	2/15: GPOs aus '{	386258C7-8072-4DCB-BF55-8631B01	09E62A}\gpreport.xml' e	einlesen						
000	3/15. GPOs ans 1/	SPOS eingelesen 31860900-3DF5-489D-B1F1-6B08F10	888F61\gpreport yml's	ainlesen						
000) -> Daten zu 1 (GPOs eingelesen	(gpreport. And	inicoch						
000	4/15; GPOS aus '{403512F7-A80E-449A-9C6A-4C7431C268D5}\gpreport.xml' einlesen									
000) -> Daten zu l (GPOs eingelesen								
000) 5/15: GPOs aus '{	4FE1C711-C682-4780-911F-0D0432E	36235}\gpreport.xml' e	einlesen						
1000) -> Daten zull	GPOs eindelesen					~			
					W.	V ALL	a sector			
					ĸ	A 1001	uch			

In der Toolbar gibt es neben der alten Schaltfläche "GPOs" auch die neue Schaltfläche "GPO-Daten", in dem die eingelesenen GPO-Einstellungen dargestellt werden:

eDoKS - lize	enzierte Vollversion - [R2301 (28	1.03.2022 10:26:41): Inhalte der Grupp	enrichtlini	en (GPOs)]					-		>
Datei F	Fenster Konfiguration Exp	ort ?								-	5
Scanir	nfo 🔄 Standardabfragen 👻	🐴 Container 👻 🗺 Vertrauensstellur	ngen -	🖪 Benutz	er 🔹 🛃 Gruppen 🕞 🗔 🤇	Computer 🔹 🕵 GPOs 👻 🐼 GPO-Daten 🔹 🖭	Server - P: Zuordn	ungen 👻 🗖 Arbei	tsplätze •		
turaneicht I				60							-
	ustenansicht	14 600-									
		16 GPOs									
en Sie eine Sp	paltenüberschrift in diesen Bereich,	, um nach dieser zu gruppieren									
OK?	Funktionstyp	Anzeigename	Be_ ak_	Co_ ak_	verlinkte Container (Anzahl)	verlinkte Container (Pfade)	Erstellt	Geändert	Einstell_ (Anzahl)	*	
🗉 🕑 ОК	Standard GPO (Microsoft)	Default Domain Controllers Polic	y 🗸	~		1 de\fiducia\ads\R2301\Domain Controllers	28.02.2018 17:41	28.02.2018 17:41		28	
🗉 🕑 ОК	Standard GPO (Microsoft)	Default Domain Policy	1	~		1 de\fiducia\ads\R2301	28.02.2018 17:41	28.02.2018 17:51		18	
🗉 🕜 OK	GPO (bankindividuell)	R2301_Test	~	~		0	28.03.2022 09:07	28.03.2022 09:14		11	
🗉 🕜 OK	GPO (bankindividuell)	R0815_ReDoKS	1	~		1 de\fiducia\ads\R2301\Admin-Root\Clients	10.02.2021 17:45	11.02.2021 20:11		6	
🗉 🕑 OK	GPO (bankindividuell)	R2301_AdminVox_Copy	~	~		1 de\fiducia\ads\R2301\Admin-Root\Clients	21.06.2020 10:54	21.06.2020 17:52		2	
🗉 🕑 OK	GPO (bankindividuell)	R2301_AdminVox_Start	~	~		1 de\fiducia\ads\R2301\Admin-Root\Benutze	er 21.06.2020 17:51	21.06.2020 17:55		1	
🗉 🕑 OK	GPO (bankindividuell)	UsrPolicy	~	~		1 de\fiducia\ads\R2301\Admin-Root\Benutze	er 17.06.2020 11:16	17.06.2020 11:16		0	
🗉 🕑 ОК	GPO (bankindividuell)	AdminRootPolicy3Cmp		~		0	17.06.2020 11:10	17.06.2020 11:13		0	
🗉 🕑 ОК	GPO (bankindividuell)	AdminRootPolicy	~	~		1 de\fiducia\ads\R2301\Admin-Root	17.06.2020 11:08	17.06.2020 11:08		0	
🗉 🕑 ОК	GPO (bankindividuell)	AdminRootPolicy5Grp1	~	~		0	17.06.2020 11:21	17.06.2020 11:22		0	
	ODO (Seallis dividuali)	A design a state for state is a			Ŧ	0	17.00 0000 11.10	17.00 0000 11.10		0	
🔍 🔽 🖡	🚽 🛛 📄 📑 📑 11 Einstel	lungen in GPO 'R2301_Test'									
Anzeigen	name	W	ert			Kategorie	Beschreibun	g			
∽ gpo							R2301_Test				
~ Comp	outerkonfiguration (cmp)						aktiviert				
✓ Skri	ipte (Scripts)										
H	lochfahren (Startup)	S	artSkript	1.cmd /t /	1						
H	lochfahren (Startup)	S	StartSkript2.cmd								
H	lerunterfahren (Shutdown)	S	ShutdownSkript1.cmd								
Herunterfahren (Shutdown)			ShutdownSkript2.cmd								
H	lerunterfahren (Shutdown)	c	test\Shu	tdownSk	ript3.cmd						
H	lochfahren (Startup)	S	artSkript	PS.cmd							
 Benutzerkonfiguration (usr) 							aktiviert				
 Skripte (Scripts) 											
A	nmeldung (Logon)	U	srStartSl	kript1.cm	t						
A	nmeldung (Logon)	U	srStartSI	kript2.cm	t						

Die obere Liste zeigt die Group Policies, die Spalte "Einstellungen (Anzahl)" enthält die Anzahl der Für die jeweilige Group Policy eingelesenen Einstellungen. In der unteren Liste werden die Einstellungen der oben ausgewählten Group Policy aufgelistet.

DoKS - lizenzierte Vollversion - [R230	1 (28.03.2022 10:26:41): Inhalte der Gruppenrichtlinien (GPOs)]	- 0	
Datei Fenster Konfiguration	Export ?	-	
🗊 Scaninfo 👩 Standardabfrager	- 🎦 Container 🔹 🚭 Vertrauensstellungen 🔹 👩 Benutzer 👻 Gruppen 🔹 🥃 Computer 🔹 💽 GPOs 🔹 💽 GPO-Da	iten 🔹 📷 Server 👻 P: Zuordnungen 👻 🔜 Arbeitsplätze 👻	
ransicht Listenansicht			
	66 Finstellungen in 16 GPOs		
n sie eine spaitenuberschrift in diesen b	reich, um nach dieser zu gruppieren		
Anzeigename (GPO)	Pfad A	Name	
Default Domain Policy	\cmp\PublicKeySettings\EFSSettings	EFSSettings	
Default Domain Policy	\cmp\PublicKeySettings\RootCertificateSettings	RootCertificateSettings	
R2301_AdminVox_Copy	\cmp\RegistrySettings\Windows-Firewall: Eingehende Portausnahmen festlegen	Windows-Firewall: Eingehende Portausnahmen festlegen Shutdown	
R2301_Test	\cmp\Scripts\Shutdown		
R2301_Test	\cmp\Scripts\Shutdown	Shutdown	
R2301_Test	\cmp\Scripts\Shutdown	Shutdown	
R2301_AdminVox_Copy	\cmp\Scripts\Startup	Startup	
R0815_ReDoKS	\cmp\Scripts\Startup	Startup	
R2301_Test	\cmp\Scripts\Startup	Startup	
R2301_Test	\cmp\Scripts\Startup	Startup	
R2301_Test	\cmp\Scripts\Startup	Startup	
Default Domain Policy	\cmp\securitySettings\clearTextPassword	ClearTextPassword	
Default Domain Controllers P.	cmp\SecuritySettings\Domänencontroller: Signaturanforderungen für LDAP-Server	Domänencontroller: Signaturanforderungen für LDAP-Server	
Default Domain Controllers P.	\cmp\SecuritySettings\Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Domänenmitglied: Daten des sicheren Kanals digital versch	
Default Domain Policy	\cmp\SecuritySettings\ForceLogoffWhenHourExpire	ForceLogoffWhenHourExpire	
Default Domain Policy	\cmp\SecuritySettings\LockoutBadCount	LockoutBadCount	
Default Domain Policy	\cmp\SecuritySettings\LSAAnonymousNameLookup	LSAAnonymousNameLookup	
Default Domain Policy	\cmp\SecuritySettings\MaxClockSkew	MaxClockSkew	
Default Domain Policy	\cmp\SecuritySettings\MaximumPasswordAge	MaximumPasswordAge	
Default Domain Policy	\cmp\SecuritySettings\MaxRenewAge	MaxRenewAge	

Hier werden die Einstellungen aller GPOs in einer Gesamtliste dargestellt. So kann leicht gesucht werden, ob z.B:

- Eine Einstellung überhaupt vorkommt und wenn ja in welcher Group Policy
- Eine Einstellung mehrfach vorkommt

Im Screenshot oben sieht man beispielsweise, dass gleich drei GPOs Startskripte definieren (und sich damit ggf. gegenseitig überschreiben).

2.1 Besonderheiten beim Vergleich von GPO-Inhalten

Wenn in der Ladekonfiguration die beiden Optionen "Vergleichsdaten laden" (zur Ausführung historischer Vergleiche) und "GPO Daten" (zum Laden von Group Policy Inhaltsdaten) aktiviert sind, dann erstreckt sich der Vergleich auch auf die Inhalte der GPOs.

Die GPO-Inhaltsdaten für die aktuellen Domänendaten werden dabei aus dem Unterverzeichnis "GPO" geladen, die für die Vergleichs-Domänendaten aus "GPO_alt".

Da die Bereitstellung der Daten in diesen Verzeichnissen manuell erfolgt kann ReDoKS nicht gewährleisten, dass die dort bereitgestellten GPO-Inhaltsdaten zeitlich zu den eingelesenen Domänendaten passen. ReDoKS kontrolliert lediglich, ob sich die Daten auf die gleiche Domäne beziehen.

10	2 R2301 Anderungen (Domäne) 23.03.2022-> 28.03.2022											
	📑 📰 💭 🕄 🍸 🙀 + 🛅 🖹 6 Änderungen (Domäne)											
Objekttyp * Anderung *												
	N	eues Objekt	Altes Objekt	geänderte Eigenschaft	neuer Wert	alter Wert						
	• ~	Objekttyp: GPO										
		 Änderung: geändert 										
		DomPolicy1	DomPolicy1	Content		F:\Data\ReDoKS\Scans\r2301\GPO_alt\Report-R2301.xml						
		Default Domain Controllers Policy	Default Domain Controllers Policy	\cmp\SecuritySettings\SeBackupPrivilege	VORDEFINIERT\Server-Operatoren (S-1-5-32-549) VORDEFINIERT\Sicherungs-Operatoren (S-1-5-32-551) VORDEFINIERT\Administratoren (S-1-5-32-544)	VORDEFINIERT\Sicherungs-Operatoren (S-1-5-32-551) VORDEFINIERT\Administratoren (S-1-5-32-544)						
		R0815_ReDoKS	R0815_ReDoKS	\cmp\Scripts\Startup		Hinzugefügt.cmd /t/1						

Außerdem kann es natürlich vorkommen, dass die bereitgestellten GPO-Inhaltsdaten unvollständig sind. Das wird beim Vergleich angezeigt, indem ein Änderungseintrag für die Eigenschaft "Content" erzeugt wird. Der darin angegebene Dateiname unter neuer/alter Wert zeigt an, aus welchen Dateien für die aktuellen Domänendaten bzw. die Vergleichs-Domänendaten Einstellungen eingelesen wurden.

Im Screenshot oben zeigt dieser Eintrag an, dass für die DomPolicy1 für die aktuellen Domänendaten keine Inhaltsdaten (im Unterverzeichnis "GPO") gefunden wurden, während für die Vergleichs-Domänendaten Inhaltsdaten in der Datei "Report-R2301.xml" (im Unterverzeichnis "GPO_alt") gefunden wurden.

Für gefundene Unterschiede wird der Pfad der Eigenschaft (siehe dazu auch Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) unter "geänderte Eigenschaft" eingetragen, so z.B. "\cmp\Scripts\Startup" für "Computereinstellungen, Skripte, Hochfahren".