ReDoKS 2.3

GPO-Detaildaten (Einstellungsinhalte) auswerten

Handbuch

Inhalt

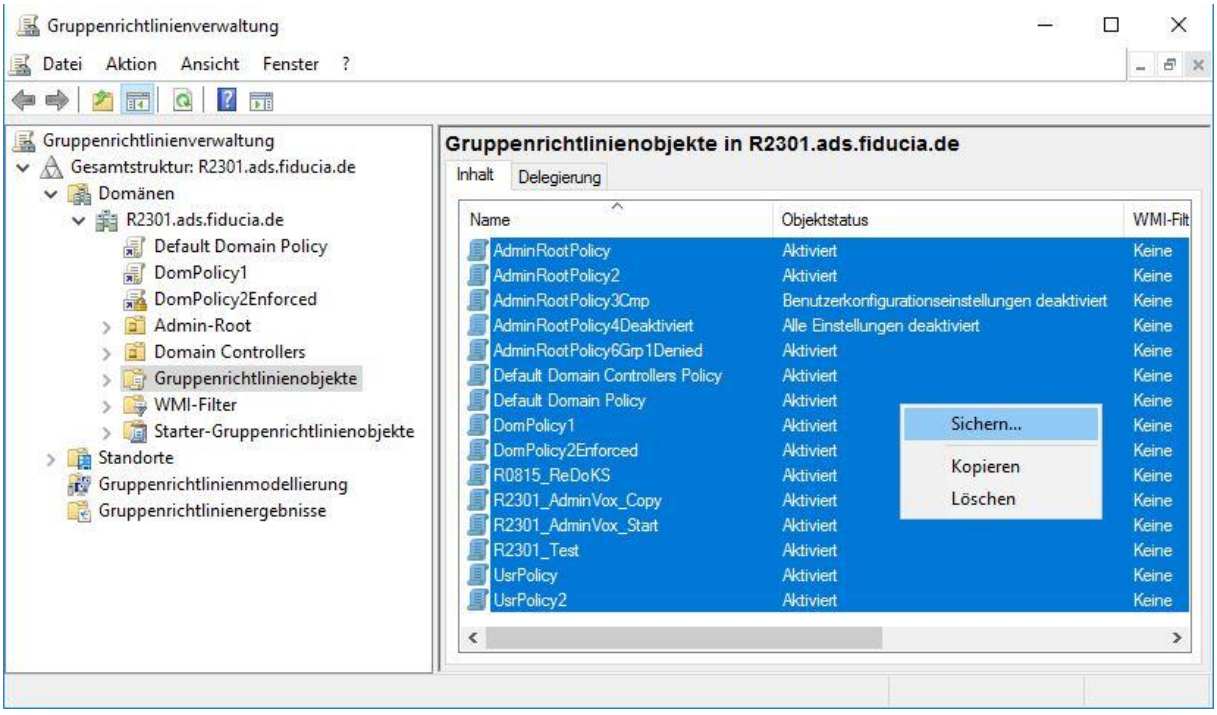
1 Ermitteln der Daten 3
1.1 Vorgehensweise bei Export über die Gruppenrichtlinienverwaltung 3
1.2 Vorgehensweise bei Export per PowerShell-Skript 4
2 Einlesen und Auswerten der Daten 4
2.1 Besonderheiten beim Vergleich von GPO-Inhalten 6

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



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”
```

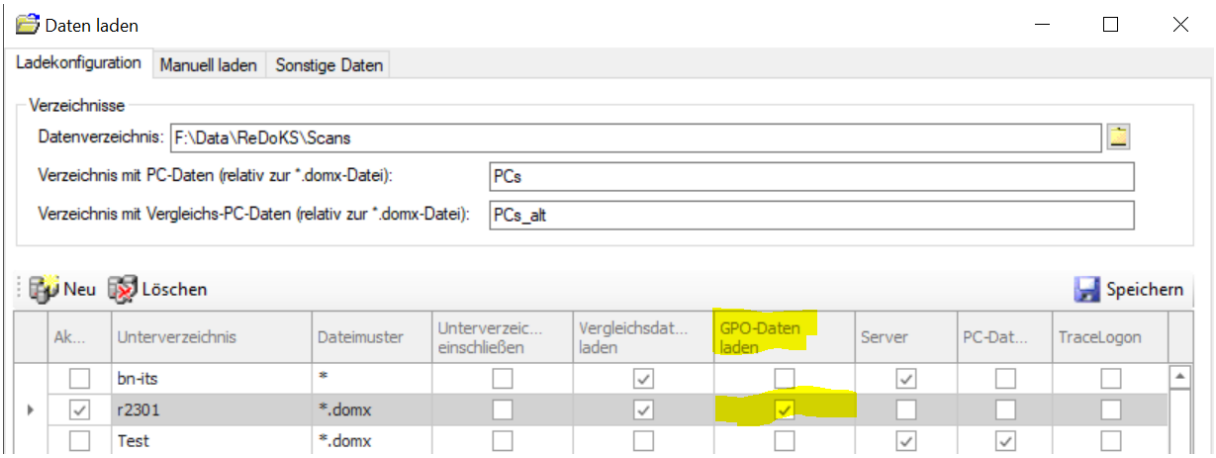
Je nach Einsatzumfeld können auch noch zwei weitere Parameter sinnvoll sein:

-domain	gibt die Domäne an, aus welcher GPOs exportiert werden sollen
-server	gibt den Domain Controller an, an den die Abfrage gerichtet wird

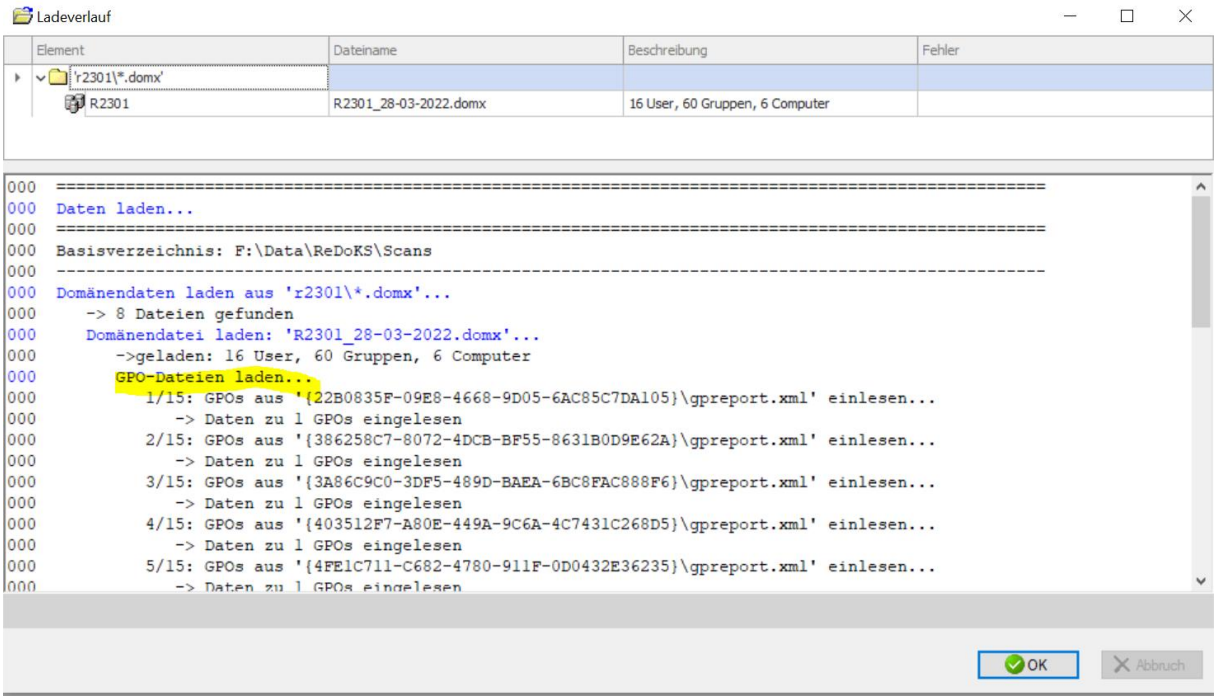
Die erzeugte(n) Datei(en) dann einfach in as Unterverzeichnis „GPO“ in dem Verzeichnis ablegen, aus dem die *.domx-Datei im Viewer eingelesen wird

2 Einlesen und Auswerten der Daten

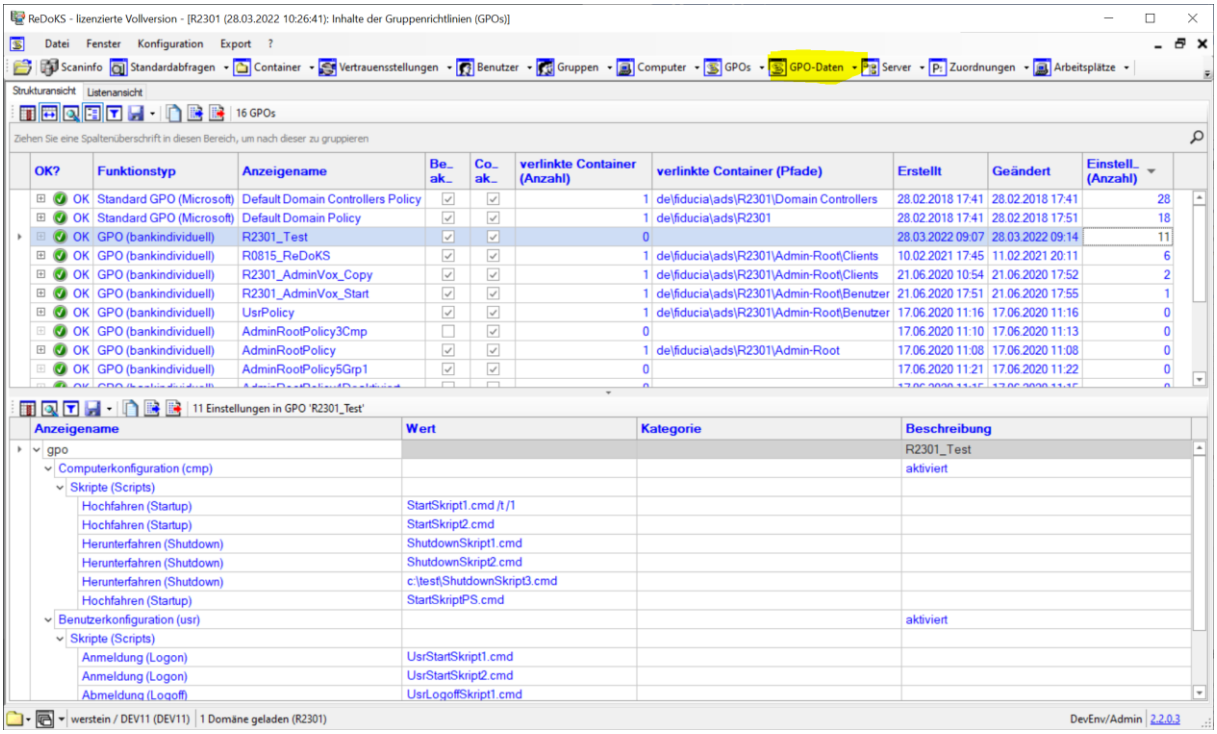
Im Ladedialog für die Domäne den Haken in der Spalte „GPO Daten“ setzen:



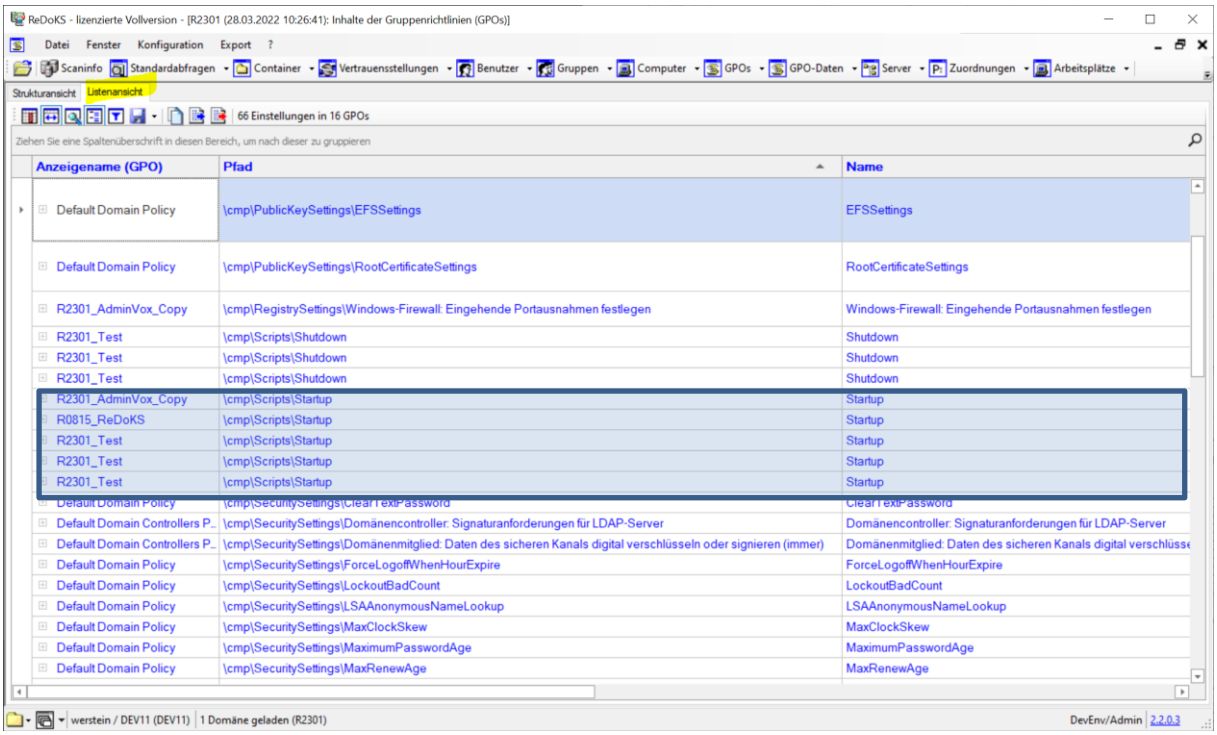
Im Ladeverlauf kommen dann entsprechende Verarbeitungsmeldungen:



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



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.



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

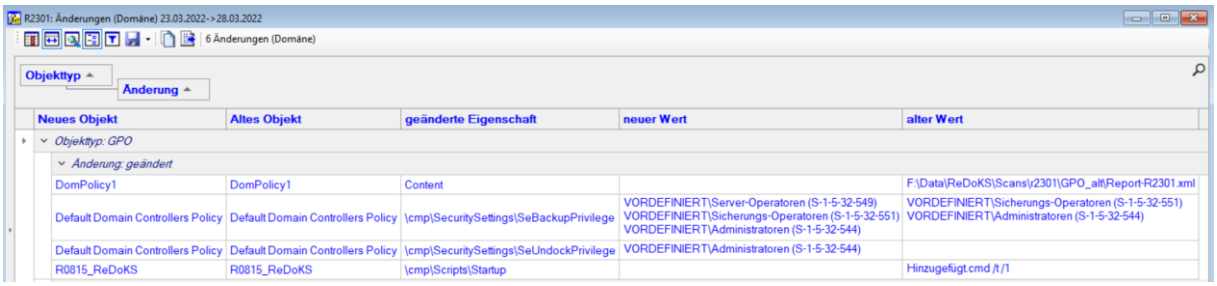
Im Screenshot oben sieht man beispielsweise, dass gleich drei GPOs Startskripte definieren (und sich damit ggf. gegenseitig überschreiben).

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.



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“.