Group Policy Best Practices

Vortrag anlässlich des 6. Treffens der WSUG L.E. am 08.02.2018

Haiko Hertes
Dipl.Inf. (FH), M.Sc.

VORGEPLÄNKEL

Domain Controller

- Egal wie klein das Unternehmen ist, zwei DCs sind Pflicht!
- Einer, mehrere oder sogar alle (seit 2012 offiziell unterstützt) dürfen virtualisiert sein
  - Dann aber nicht alle VMs auf einem Host laufen lassen!
- Bei mehreren Niederlassung: Ggf. min. einen DC pro Niederlassung
- Selbiges gilt im Prinzip für DNS

Domain Controller

- Statische IP-Adresse
- DNS „über Kreuz“
  - DC der auch DNS-Server ist soll sich selbst als letztes benutzen
- Korrekte Uhrzeit
  - Oder: wenn falsch, dann überall gleich falsch!
  - PDC-Emulator gegen externe Zeitquelle synchronisieren

Domain Controller

- Domain Controller sind „heilige Maschinen“ und sollten in erster Linie DCs sein
- Ggf. zusätzlich DHCP, DNS, CertSrv
- Keinesfalls zusätzlich Fileserver, Mailserver, Application Server oder andere „Eierlegendewollmilchsäue“
  - Ausnahme: SBS – da ist das quasi „gewollt“

Domänenname

- Der Domänenname sollte gut überlegt sein – Änderungen sind sehr aufwändig!
- Sind das gute Domänennamen?
  - domain.local
  - company.intern
  - mycorp.com
- Besser:
  - ad.mycorp.com
- Dann als NetBIOS Namen aber nicht „AD“ sondern „MYCORP“ verwenden!

FSMO-Rollen

- „Flexible Single Master Operations“ bzw. „Betriebsmaster“
  - Domain Naming Master
  - Schema-Master
  - RID (Relative ID)-Master
  - PDC (Primary Domain Controller)-Emulator
  - Domain Infrastructure Master
- „übergeben“ vs. „übernehmen“

1x/Forest

1x/Domain

Sicherheit

- Physischen Zugang zu DCs schützen
- Logischer Zugang ist per default auf Domain Admins beschränkt und sollte es auch bleiben
  - Anzahl der Domain Admins auf notwendiges Maß begrenzt halten
  - Domain Admin Accounts nicht für andere Zwecke nutzen
- Einsatz von RODC und Server Core

RODC

- Read-only DC
- Unidirektionale Replikation
  - Schreibende Änderungen müssen an regulären DC weitergeleitet werden
- Passwortreplikation steuerbar
- Ideal für kleine Außenstellen

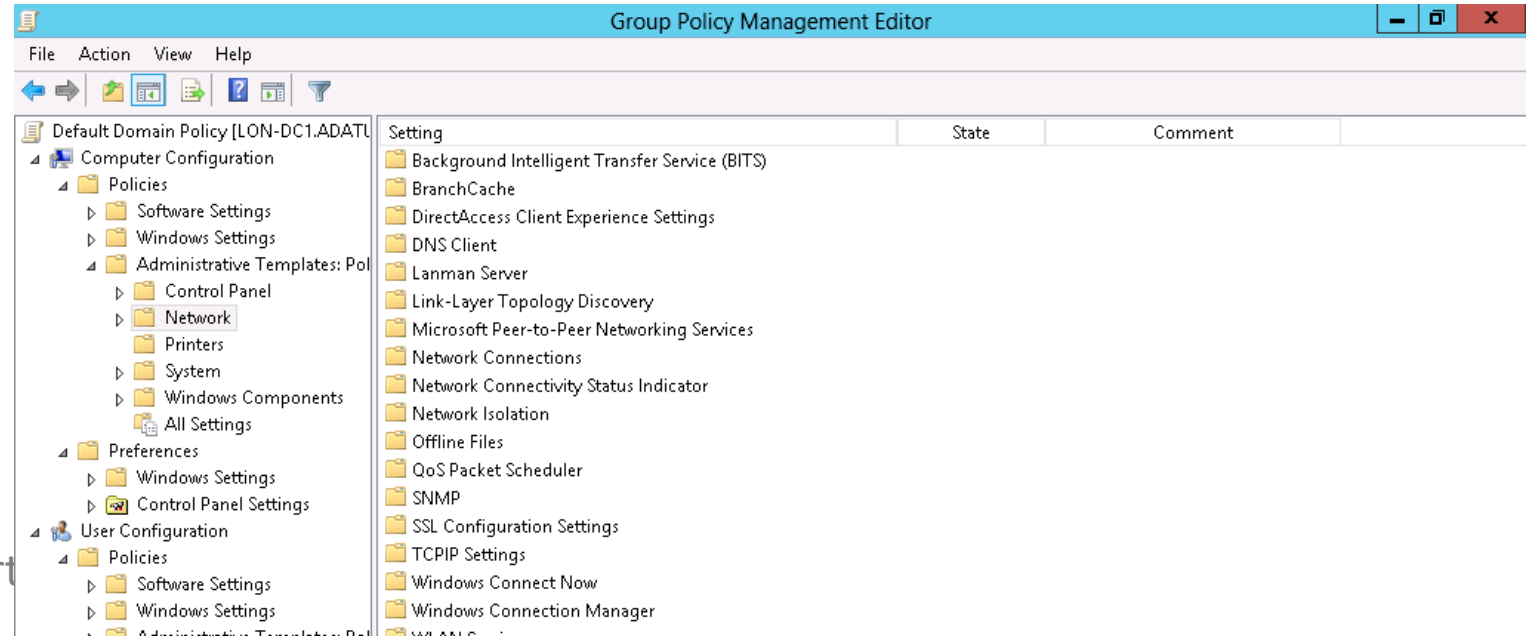
GROUP POLICIES

Allgemeines

- Group Policies sind Vorgaben oder Voreinstellungen, die ein Administrator für die Geräte und Benutzer einer Domain festlegen kann
- Sie gelten i.d.R. im „Wirkungsbereich“ für jeden
- Wirkungsbereich kann eingeschränkt werden

Allgemeines

- Die einzelnen Einstellungen sind in GPOs, Group Policy Objects, niedergeschrieben
- Jede GPO erhält nach dem Anlegen alle Möglichkeiten, von denen aber noch keine aktiviert ist; damit ist die GPO in der Wirkung faktisch „leer“

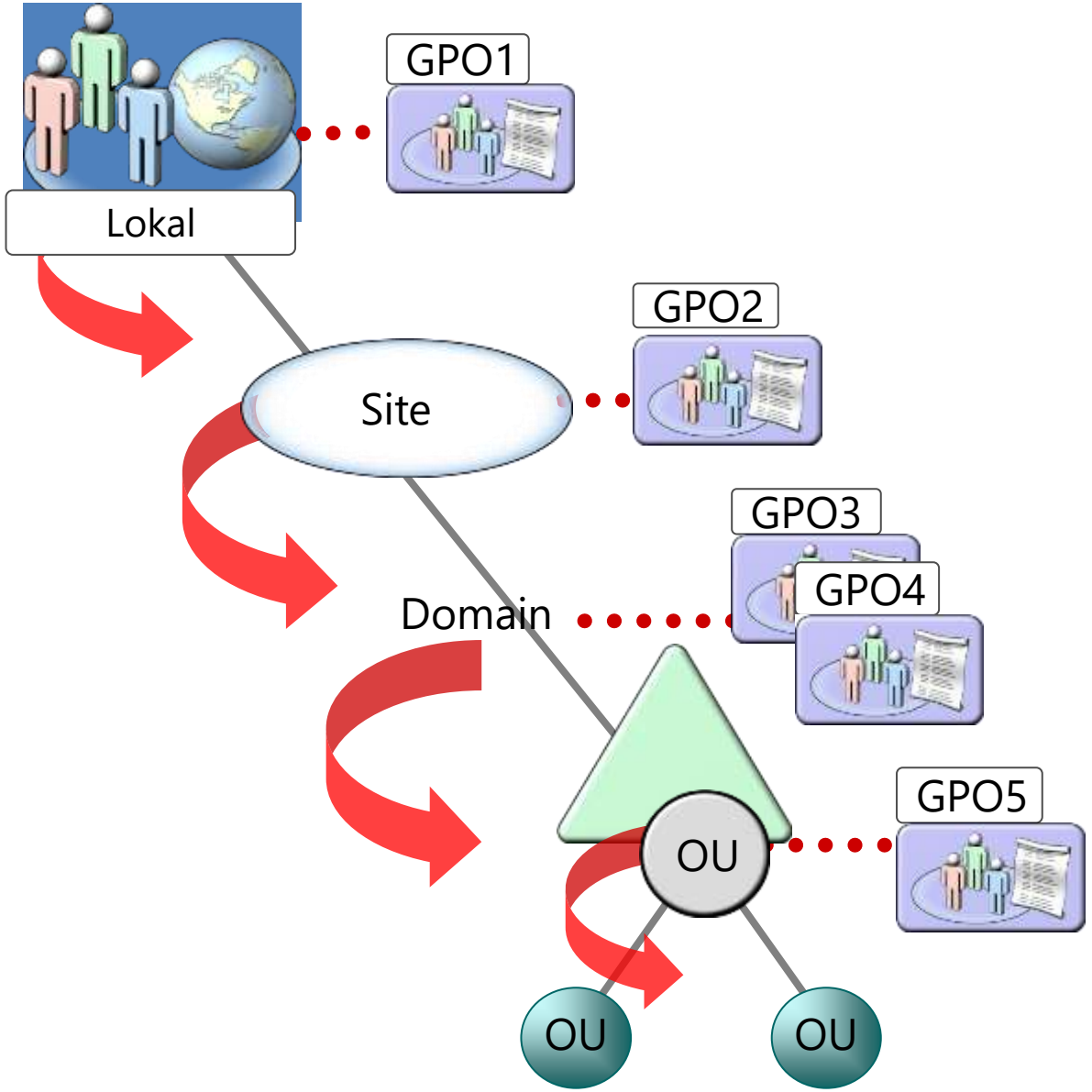


Wirkungsbereich

- Damit eine GPO wirken kann, muss sie mit ihrem Wirkungsbereich „verknüpft“ werden
- Dabei bieten sich 3 Möglichkeiten:
  - Gesamte Domäne
  - Einzelne oder mehrere Organisationseinheiten (OUs)
  - AD-Standorte
- Eine GPO kann nicht (direkt) mit einer Gruppe oder gar einem Einzelgerät verknüpft werden!

Wirkungsbereich

- GPOs werden auf untergeordnete OUs vererbt (wenn Vererbung nicht deaktiviert wurde)
- Dabei gelten Regeln, welche GPO bei Widerspruch Vorrang hat
- Wirkungsbereich lässt sich weiter beeinflussen:
  - Sicherheitsfilter
  - WMI-Filter
  - Deaktivierte Vererbung
  - Erzwingen



Wirkungsbereich

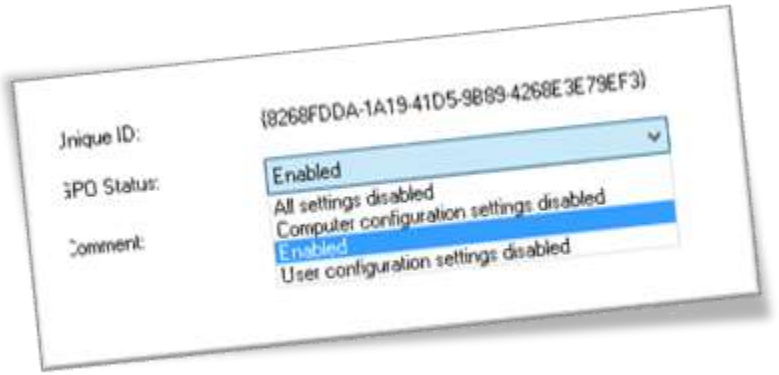
- Die OU ist das gängigste Mittel, die Wirkung von GPOs zu steuern
- Daraus folgt: Strukturierung der OUs folgt dem später gewünschten Einsatz von GPOs
- Da Container auf dem direkten Weg keine OUs enthalten können und auch keine GPOs verknüpft werden können: CN=Computers und CN=Users nicht nutzen!

Wirkungsbereich

- Da ein AD-Objekt (Benutzer / Computer) nur an EINEM Ort gespeichert sein kann, sind parallel Gliederungen nicht sinnvoll (z.B. nach Standort, parallel nach Abteilung und dann nochmal nach Aufgabe)
  - Sinnvoll ist aber eine Gliederung „vom Groben zum Feinen“, als z.B. auf oberster Ebene alle Standorte, darunter die jeweiligen Abteilungen und so weiter
  - GPOs lassen sich auch problemlos mehrfach verknüpfen!

Wirkungsbereich

- Ein GPO enthält Einstellmöglichkeiten für Computer UND Benutzer
- Für bessere Übersicht und weil die Objekte im AD idR sowieso getrennt sind sollte eine GPO nur Einstellungen für Benutzer ODER Computer setzen
- Nicht benutzter Teil kann deaktiviert werden!



Wirkungsbereich

- Egal wo und wie GPOs verknüpft sind:
  - Computerrichtlinien wirken nur auf Computerobjekte der Domäne und Benutzerrichtlinien nur auf Benutzerobjekte
  - Wenn anders nötig: Loopbackverarbeitung nutzen! (z.B. bei Terminalservern: Benutzerkonten sollen bestimmte Einstellungen haben, dies soll aber nur auf die Terminalserver wirken)

Struktur

- OU „Domain Controllers“ belassen, wie sie ist, wenn es keine Gründe zur Änderung gibt!
- Default Container für Computer und Benutzer „umbiegen“ (`redircmp` / `redirusr`)
- OUs frühzeitig in Benutzer und Computer splitten

Neue GPOs

- „Sprechende“ Namen
  - Knapp halten
  - Nicht: „Was will ich mit der GPO erreichen?“ sondern: „Was tut die GPO?“
  - Bsp.: „CPR-FirewallAufAllenServernAbschalten“ vs. „CPR-FirewallAbschalten“
- Ggf. gleich im Namen erkennbar, ob Computer- oder Benutzer-GPO
- Jede GPO nur für einen Zweck verwenden, nicht vermischen
- Vor der Anwendung an großen Nutzerkreisen testen

Neue GPOs

- Deaktivieren der Vererbung und Erzwingen einer GPO sehr sparsam verwenden!
- Wenn GPO auf User(gruppen) gefiltert wird:
  - Nicht vergessen, den/die nötigen Computer lesend zu berechtigen!

Nicht mehr benötigte GPOs

- Im Sinne der Übersichtlichkeit regelmäßig „aufräumen“
- GPOs aber am besten nie sofort löschen
  - Zunächst nur Verknüpfung deaktivieren, später Verknüpfung löschen
    - Dadurch lässt sich die GPO bei Problemen schnell wieder reaktivieren
  - Wenn keine Probleme auftreten und die GPO endgültig weg soll, kann man sie dann später löschen

Erreichbarkeit

- https://about.me/haiko.hertes
- https://www.hertes.net
- https://www.youtube.com/user/SilentDeath86/feed
- https://www.xing.com/profile/Haiko_Hertes

Fragen und offene Punkte