



Gruppenrichtlinienupdate per Powershell erzwingen

Das Erstellen, anlegen und verwalten von Gruppenrichtlinien, lässt sich ganz einfach per Powershell erledigen.

In diesem Dokument geht es um die (remote) Erzwingung eines Gruppenrichtlinienupdates auf Maschinen einer definierten OU.

Für die Ausführung wird nicht viel benötigt außer, dass Recht die Maschinen administrieren zu dürfen.

Das Powershell Skript ist schlank aber effektiv.

```
# Ein GPOupdate auf alle Maschinen anwenden aus der OU...
Get-ADComputer -filter * -SearchBase "OU=2016,OU=Machines,OU=ORG,DC=ndsedv,DC=de" |
  ForEach-Object -Process {
    Invoke-GPOupdate -Computer $_.name -Force
  }

# Domänennamen in eine Variable setzen
$DomainDN = (Get-ADDomain).distinguishedName

# Ein GPOupdate auf alle Maschinen anwenden aus der OU...
Get-ADComputer -filter * -SearchBase "CN=Computers,$DomainDN" |
  ForEach-Object -Process {
    Invoke-GPOupdate -Computer $_.name -Force
  }
```

The screenshot shows the Windows PowerShell ISE interface. The script content is as follows:

```
1 # Domänennamen in eine Variable setzen
2 $DomainDN = (Get-ADDomain).distinguishedName
3
4 # Ein GPOupdate auf alle Maschinen anwenden aus der OU...
5 Get-ADComputer -filter * -SearchBase "OU=2016,OU=Machines,OU=ORG,DC=ndsedv,DC=de" |
6 # Get-ADComputer -filter * -SearchBase "CN=Computers,$DomainDN" |
7   ForEach-Object -Process {
8     Invoke-GPOupdate -Computer $_.name -Force
9   }
10
11
```

The console output shows the execution of the script:

```
PS C:\Windows\system32> # Ein GPOupdate auf alle Maschinen anwenden aus der OU...
Get-ADComputer -filter * -SearchBase "OU=2016,OU=Machines,OU=ORG,DC=ndsedv,DC=de" |
# Get-ADComputer -filter * -SearchBase "CN=Computers,$DomainDN" |
  ForEach-Object -Process {
    Invoke-GPOupdate -Computer $_.name -Force
  }

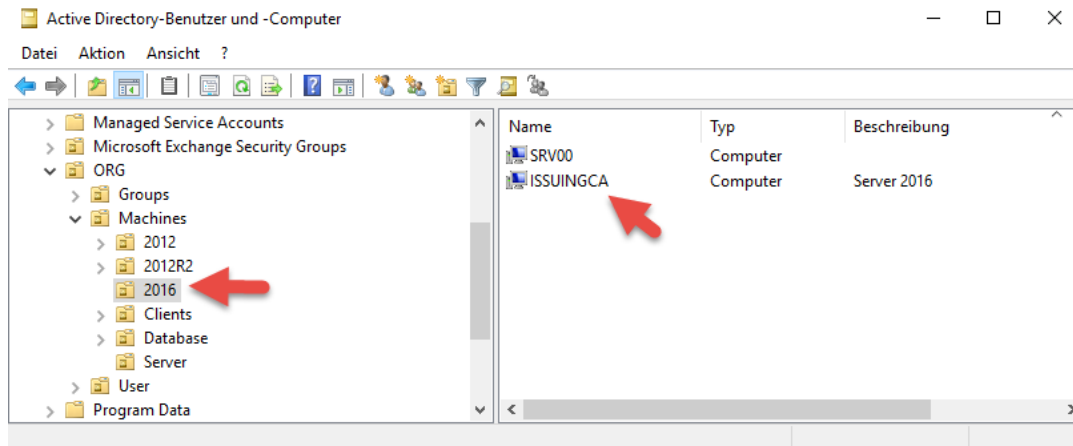
PS C:\Windows\system32>
```

The status bar at the bottom indicates "Abgeschlossen" (Completed) and "Ln 4 Spalte 1" (Line 4, Column 1).

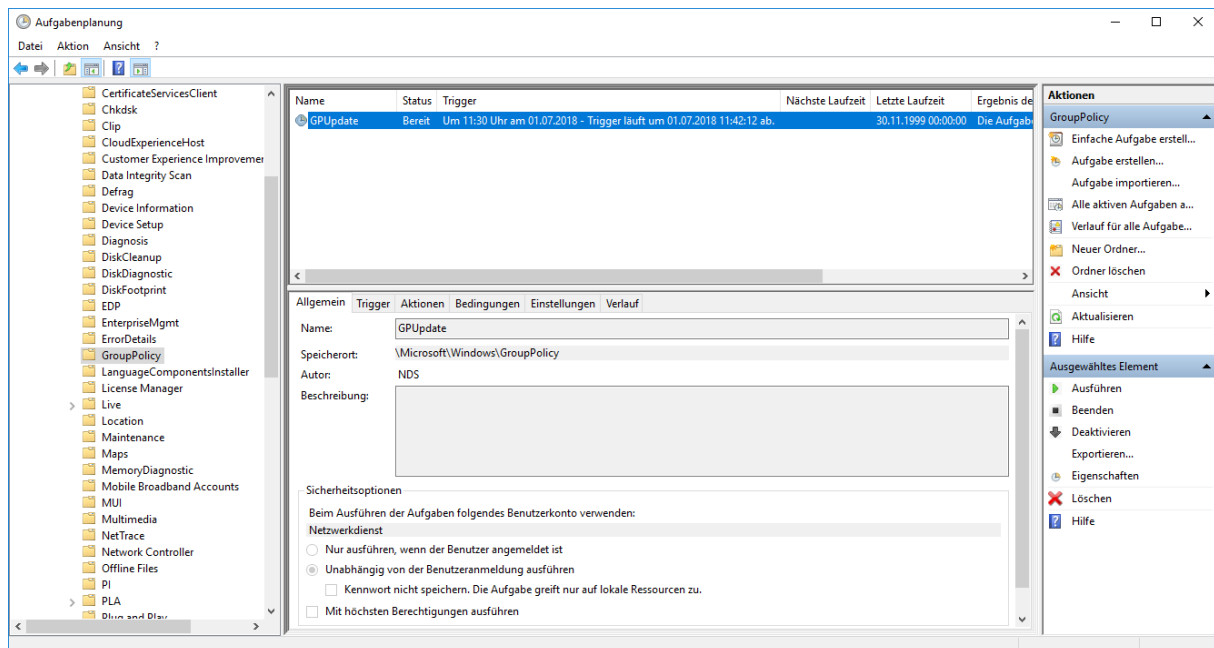


Gruppenrichtlinienupdate per Powershell erzwingen

Der Befehl wurde auf die Maschinen ausgeführt die sich in der OU „2016“ befinden.



Schauen wir uns daraufhin mal die lokale Aufgabenplanung auf dem Server ISSUINGCA an. Hier ist klar zu erkennen, dass die Aufgabe 11:42 ausgeführt wird





Gruppenrichtlinienupdate per Powershell erzwingen

Die Aktion die stattfinden soll ist die die wir übermittelt haben und zwar ein gpupdate /force.

The screenshot shows the Windows Task Scheduler console. The task 'GPUUpdate' is selected, and the 'Allgemein' (General) tab is active. The 'Name' column shows 'GPUUpdate', 'Status' is 'Bereit' (Ready), and the 'Trigger' is set to 'Um 11:30 Uhr am 01.07.2018 - Trigger läuft um 01.07.2018 11:42:12 ab.' The 'Nächste Laufzeit' (Next Run Time) is '30.11.1999 00:00:00' and the 'Ergebnis der letzten Ausführung' (Last Run Result) is 'Die Aufgabe wurde erfolgreich ausgeführt' (Task completed successfully). The 'Aktionen' (Actions) tab is also visible, showing a single action: 'Programm starten' (Start program) with details 'gpupdate.exe /target:computer /force'. A red box highlights this action.

Ein weiterer Blick in den Verlauf zeigt uns wann die Aufgabe registriert wurde:

The screenshot shows the Windows Task Scheduler console with the 'Verlauf' (History) tab selected. It displays a list of events for the task 'GPUUpdate'. The table below summarizes the events:

Ebene	Datum und Uhrzeit	Ereignis-ID	Aufgabenkategorie	Vorgangscod	Korrelations...
Informati...	01.07.2018 11:30:12	140	Die Aufgabenregistrierung wurde aktualisiert.	Info	
Informati...	01.07.2018 11:30:12	106	Aufgabe registriert	Info	
Informati...	10.09.2017 22:59:55	141	Die Aufgabenregistrierung wurde gelöscht.	Info	
Informati...	10.09.2017 20:08:36	140	Die Aufgabenregistrierung wurde aktualisiert.	Info	
Informati...	10.09.2017 20:08:36	106	Aufgabe registriert	Info	

Below the table, the details for event ID 140 are shown. The message states: 'Die Aufgabe "Microsoft\Windows\GroupPolicy\GPUUpdate" wurde vom Benutzer "S-1-5-20" aktualisiert.' (The task "Microsoft\Windows\GroupPolicy\GPUUpdate" was updated by user "S-1-5-20"). Additional details include: 'Protokollname: Microsoft-Windows-TaskScheduler/Betriebsbereit', 'Quelle: TaskScheduler', 'Protokolliert: 01.07.2018 11:30:12', 'Ereignis-ID: 140', 'Aufgabenkategorie: Die Aufgabenregistrierung wurde aktualisiert.', 'Ebene: Informationen', 'Schlüsselwörter:', 'Benutzer: SYSTEM', 'Computer: IssuingCA.ndsedv.de', and 'Vorgangscod: Info'.



Gruppenrichtlinienupdate per Powershell erzwingen

Springen wir nun vom Taskplaner in die Ereignisanzeige. Hier finden wir die Person, die den Befehl abgesetzt hat, bzw. den Task geplant hat.

The screenshot shows the Windows Event Viewer window titled 'Ereignisanzeige'. The left pane shows the tree view with 'Betriebsbereit' selected. The main pane displays a list of events for 'Betriebsbereit' with 5336 total events. The selected event (ID 5017) is highlighted. The details pane shows the following information:

Protokollname:	Microsoft-Windows-GroupPolicy/Betriebsbereit		
Quelle:	GroupPolicy (Microsoft-Win	Protokolliert:	01.07.2018 11:30:34
Ereignis-ID:	5017	Aufgabenkategorie:	Keine
Ebene:	Informationen	Schlüsselwörter:	
Benutzer:	NSSEDEV\NDS	Computer: <td>IssuingCA.ndsedv.de</td>	IssuingCA.ndsedv.de
Vorgangscod:	Info		

The screenshot shows the Windows Event Viewer window titled 'Ereignisanzeige'. The left pane shows the tree view with 'Betriebsbereit' selected. The main pane displays a list of events for 'Betriebsbereit' with 5336 total events. The selected event (ID 5310) is highlighted. The details pane shows the following information:

Protokollname:	Microsoft-Windows-GroupPolicy/Betriebsbereit		
Quelle:	GroupPolicy (Microsoft-Win	Protokolliert:	01.07.2018 11:30:34
Ereignis-ID:	5310	Aufgabenkategorie:	Keine
Ebene:	Informationen	Schlüsselwörter:	
Benutzer:	SYSTEM	Computer: <td>IssuingCA.ndsedv.de</td>	IssuingCA.ndsedv.de
Vorgangscod:	Info		

Das war's auch schon.

- GPUupdate remote planen und ausführen
- Task lokal kontrolliert
- Die Ereignisanzeige gibt Aufschluss wer den Task durchgesetzt hat

Eine einzelne Maschine zum gpupdate /force zwingen:

Invoke-GPUupdate -Computer SRV00