**Ablauf Practical Day**

Sie werden in den nächsten 3 Lektionen weitere Servertools und Rollen kennenlernen, welche in der Systemtechnik verwendet werden.

**Support Tools 30 Min**

In der Regel arbeitet der Systemtechniker nicht direkt vor Ort physikalisch am Serversystem. Es gibt entsprechende Remote oder Fernwartungstools, welche für die Installation/Konfiguration und Support verwendet werden können.

Ich habe Ihnen einen Auszug einiger Remote Tools hinzugefügt. Schauen Sie sich diese Tools an und versuchen Sie zu zweit oder Alleine die Tools nutzen zu können.

Sie benötigen für die folgenden Tools eine Internetverbindung. Verwenden Sie dazu Ihr Notebook oder eine Windows 10 VM, welche Internetzugang besitzt.

* Teamviewer
* VNC
* UltraVNC

Für die nachfolgenden Tools benötigen Sie keine Internetverbindung. Verwenden Sie dazu Ihre virtuelle Serverumgebung. Installieren Sie auf dem Client die RDP Tools und richten Sie die Verbindung zum WDS oder Domaincontroller ein.

* Remote Desktop Manager
* mRemote NG
* ASG Remote Desktop

**Auftrag**

Versuchen Sie die wichtigsten Unterschiede festzuhalten.

**Serverinformationen und Fehlereventlog 30 Min**

**Ereignisanzeige**

Im Windowsumfeld gibt es eine Ereignisanzeige für jegliche Events unter Windows. Es gibt Standardbereiche (System, Sicherheit und Anwendung). In der Regel können hier die wichtigsten Events ausgelesen werden und analysiert werden.

Neben diesen Standardbereichen können auch für die einzelnen Dienste entsprechende Logs ausgelesen werden.

**Sie finden dazu Unterlagen auf Teams (M123\_12\_Ereignisanzeige.docx).**

Schauen Sie sich das folgende Tool einmal an:

<http://www.nirsoft.net/utils/my_event_viewer.html>

Mit diesem Tool können Sie die lokale Ereignisanzeige auslesen und auch via Remote entsprechende Logs auslesen, sofern Sie die richtigen Berechtigungen besitzen (Domain Admins).

Sie können dazu auch das **Windows Server Manager** verwenden.

Sie finden hier pro installierte Rolle die wichtigsten Tools, das Eventlog auf diese Rolle bezogen und einen Best Practice Analyzer (BPA).

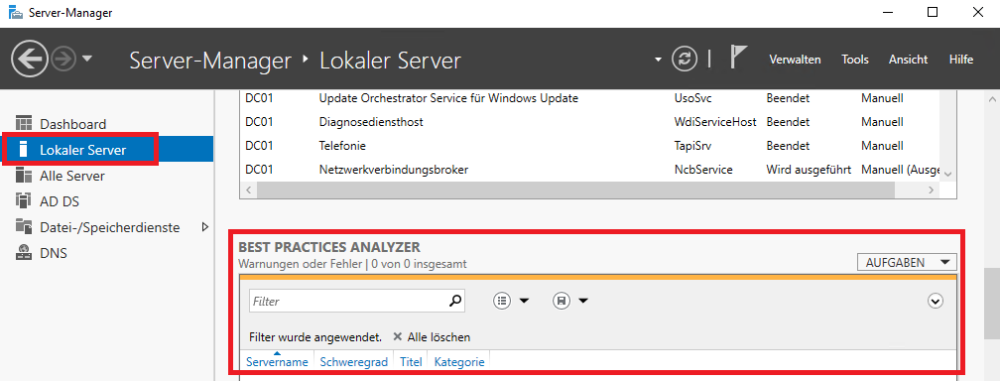
<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager>

Schauen Sie sich einmal den BPA bei Active Directory an.

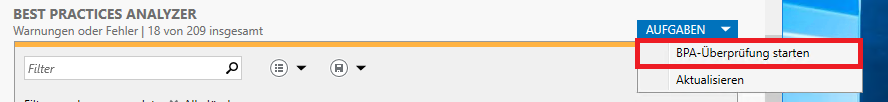
In diesem Abschnitt möchte ich mir den Best Practices Analyzer unter Windows Server 2016/2019 näher ansehen. Meiner Erfahrung nach wird der BPA wenig bis gar nicht benützt. Alles muss schnell gehen, die nächste Aufgabe wartet schon, wozu sich mit Microsoft Empfehlungen herumschlagen? Dabei liefert er doch wertvolle Informationen zur Optimierung des Systems.

## BPA im Server-Manager

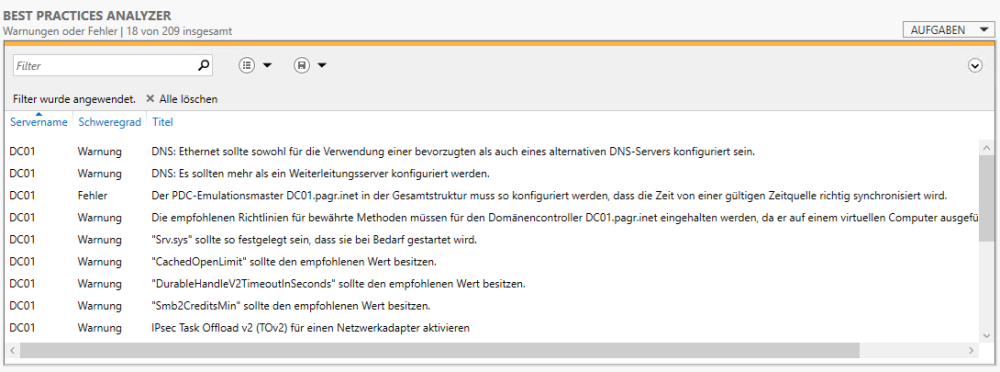
Der BPA ist im Server-Manager unter Lokaler Server zu finden.



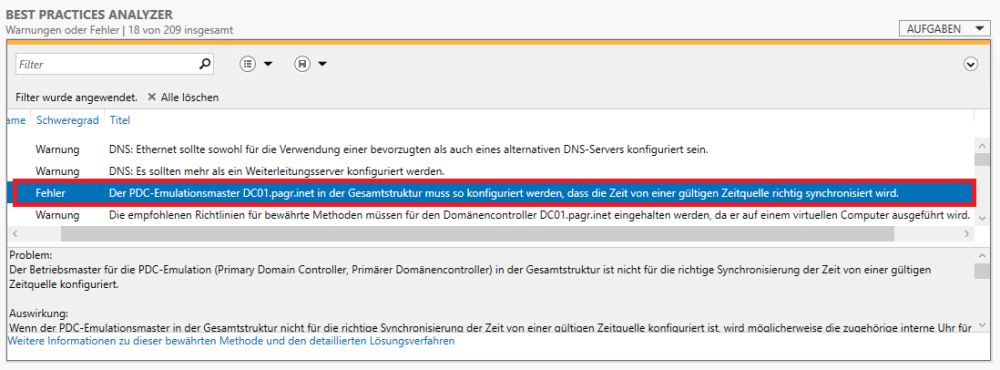
Klickt man auf AUFGABEN und auf BPA-Überprüfung starten dann gehts los.



Die Ergebnisse trudeln ein, und zwar eine ganze Menge.



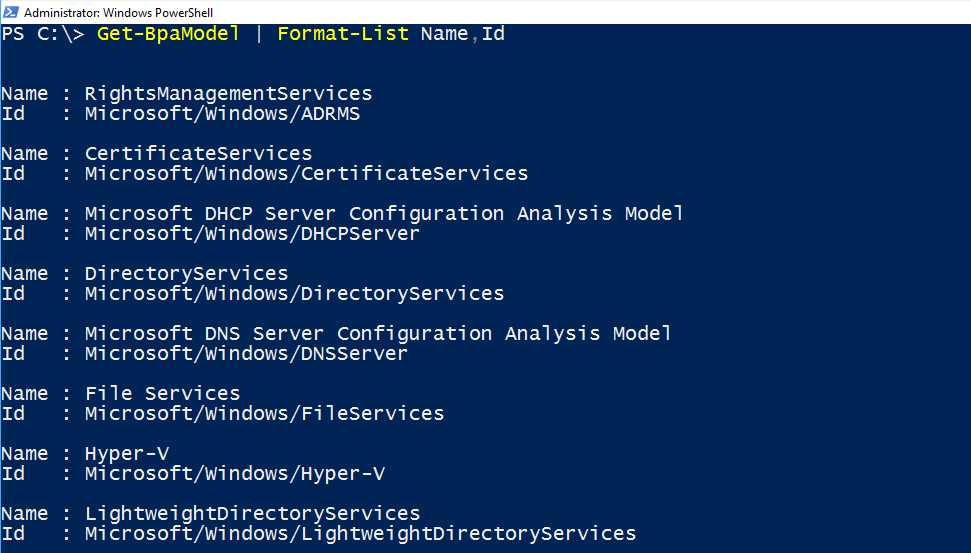
Mein Server wurde kurz zuvor zum Domain-Controller hochgestuft und schon meldet der BPA, dass ich gefälligst eine zuverlässige Zeitquelle für den PDC Master konfigurieren soll. Der PDC Master ist der Zeitgeber der Domäne.  Man spricht hier auch von [Active Directory FSMO Rollen (Betriebsmaster)](https://sid-500.com/2017/02/11/active-directory-fsmo-rollen-betriebsmaster/).



## BPA in PowerShell

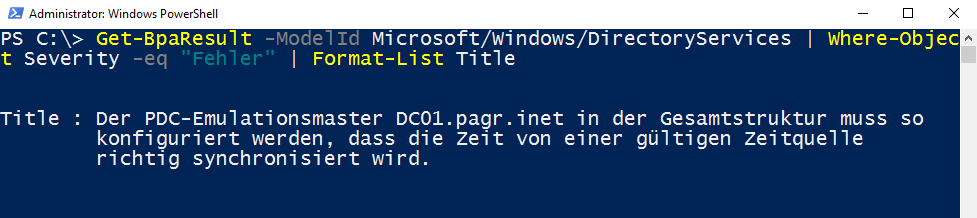
In PowerShell ist das Ganze noch übersichtlicher, zumindest dann, wenn man die Ergebnisse filtert. In meinem Fall möchte ich nur die BPA Ergebnisse in Bezug auf Active Directory Domänendienste sehen und dazu brauche ich die Id.

**Get-BpaModel | Format-List Name,Id**



Die Id lautet also Microsoft/Windows/DirectoryServices. Dann rufe ich die BPA Ergebnisse eben dieser Id ab, und zwar nur die Fehler.

**Get-BpaResult -ModelId Microsoft/Windows/DirectoryServices | Where-Object Severity -eq "Fehler" | Format-List Title**



**Laborübung 60 Min**

**Lernziele**

Die Teilnehmer können eine Kundensituation gemäss Vorgaben umsetzen. Dabei werden die gelernten Komponenten wie AD, DNS, DHCP eingesetzt.

**Art der Aufgabe**

Gruppenarbeit, 2er Gruppe

**Ausgangslage**

Sie bekommen einen Kundenauftrag, indem Sie ein neues Netzwerk aufbauen müssen.

Der Kunde möchte neu ein Active Directory mit zwei Domänencontroller einsetzen.

Überlegen Sie einmal, welche Rollen sollten in der Praxis redundant ausgelegt sein und wieso:

Weiter sollten noch bestimme Netzwerkdienste auf den einzelnen Servern konfiguriert werden.



Verwenden Sie als Hauptserver Ihren bestehenden Domaincontroller.

Erstellen Sie für den weiteren Domaincontroller eine neue virtuelle Maschine.

**Zusätzliche Funktion**

**DHCP**

Installieren Sie auf jedem Domain Controller einen DHCP

Scope 1 192.168.x.120 – 192.168.x.149

Scope 2 192.168.x.150 – 192.168.x.199

**Windows Backup als Dienst einrichten und konfigurieren**

Erstellen Sie vom Windows Server MYADDC01 eine Sicherung auf das Laufwerk D.

<https://www.windowspro.de/wolfgang-sommergut/windows-server-sicherung-installation-funktionen-einschraenkungen>

**Hinweis:**

Achten Sie auf die IP Adressen und Subnetmasken.

**Optional**

Schauen Sie sich die folgenden Features unter Windows Server und 10 an.

Docker

Linux Subsystem