Eigener PowerShell Benutzer für Sensoren (Exchange)

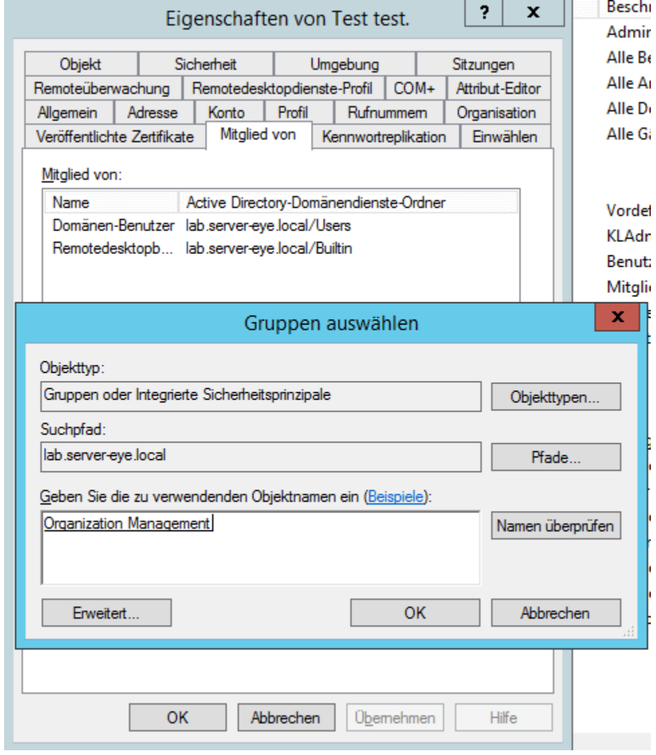
Normalerweise ist der beste/einfachste Weg zur Nutzung einer **Remote-PowerShell** für Server-Eye der **Domänenadministrator**. Hierdurch sind **alle Berechtigungen** schon gesetzt und es sollte zu keinem Problem kommen. Wollen Sie aber einen **einfachen Benutzer** für die PowerShell Nutzung anlegen, gibt es hier eine **Basis-Anleitung** zur Erstellung.

Als Beispiel nehmen wir den **Exchange Gesundheit** Sensor, wo die Notwendigkeit der Eingabe von Nutzerdaten am häufigsten auftreten wird (ab 2013). Dabei unterteilt die folgende Anleitung den Prozess in mehrere Schritte die hier zur Übersichtlichkeit aufgelistet sind:

- **Voraussetzungen** für **Exchange**
- PowerShell **Berechtigungen** am **Endpoint**
- Spezielle **WMI Berechtigungen**
- **Dienstberechtigungen**
- **Testlauf**

Schritt 1 – Voraussetzungen für Exchange

Anfänglich muss für die **Exchange Sensoren** noch folgende **Gruppenzugehörigkeit** hinzugefügt werden, damit eine Berechtigung zur Verwaltung vorliegt. Die Gruppe ist „**Organization Management**“

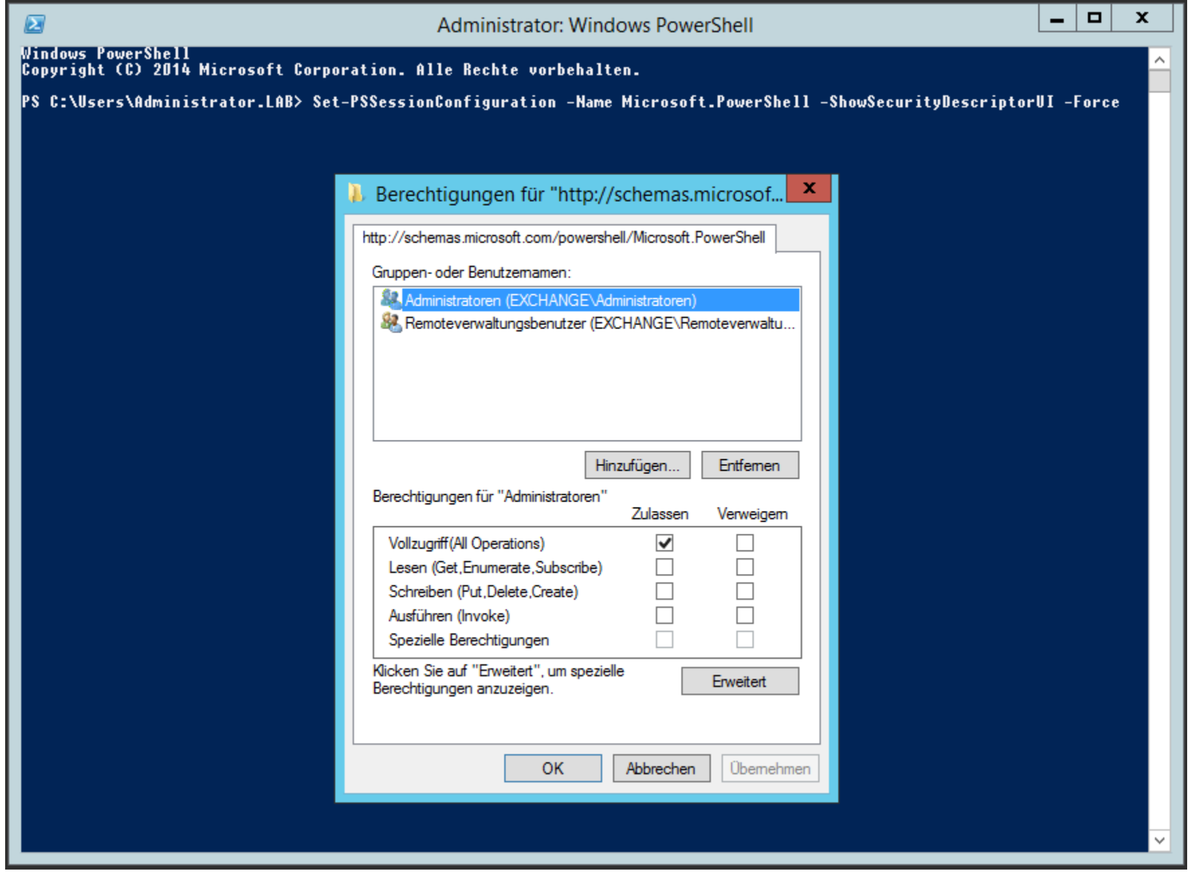


Denn fehlt diese, kann es später bei der Anmeldung zum Fehler „**Benutzer xyz ist keiner Verwaltungsrolle zugewiesen**“ kommen.

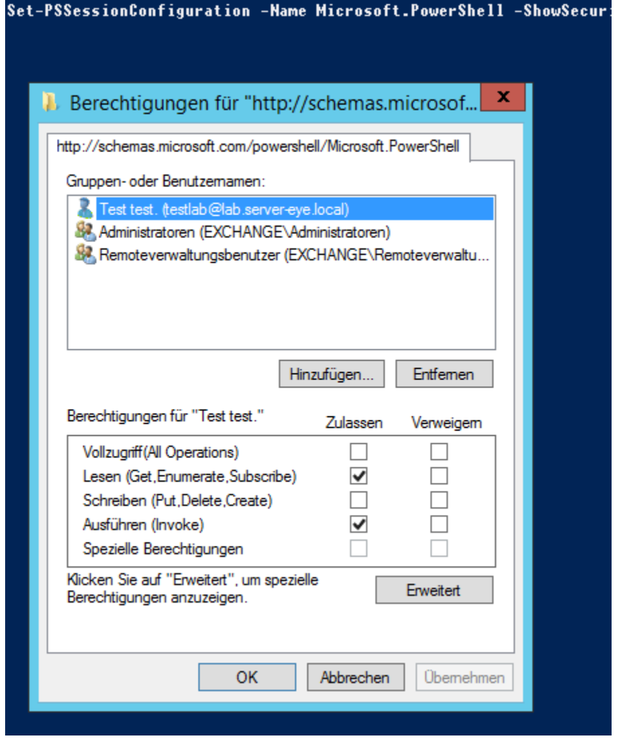
Schritt 2 – PowerShell Berechtigungen am Endpoint

Diese Änderungen müssen auf dem System durchgeführt werden, wohin eine Verbindung aufgebaut werden soll. Starten Sie dazu die **PowerShell als Administrator** und geben Sie folgenden Befehl ein:

- *Set-PSSessionConfiguration -Name Microsoft.PowerShell -ShowSecurityDescriptorUI -Force*



Dabei müssen Sie explizit die Berechtigungen „**Lesen**“ und „**Ausführen**“ vergeben.

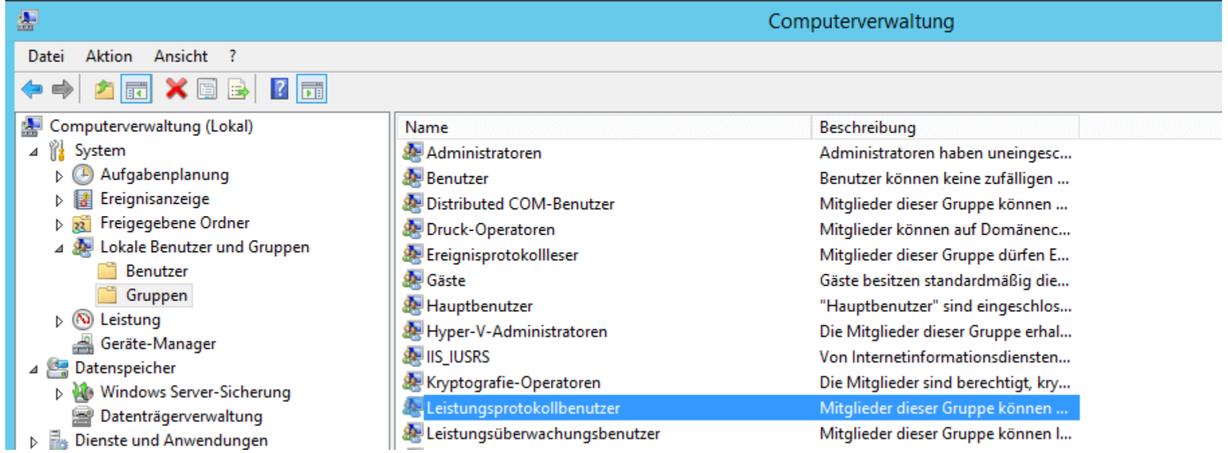


Bei weiteren Fragen hierzu können Sie auch den Blog Artikel von Microsoft nutzen.

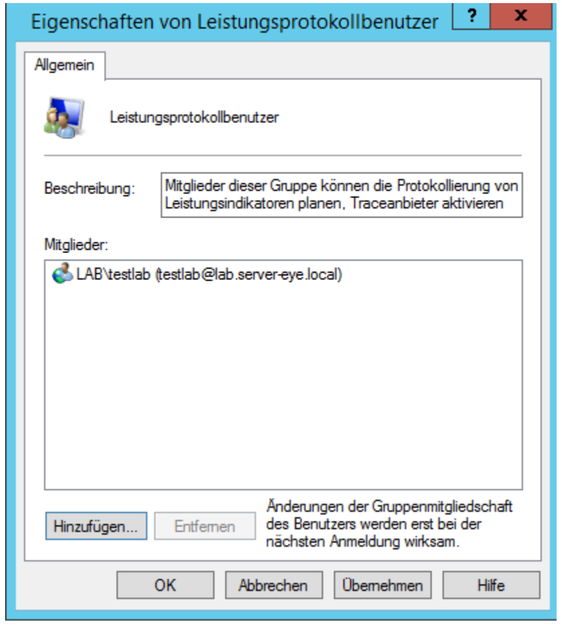
Schritt 3 – WMI Berechtigungen

Da viele Zugriffe in der **PowerShell** intern auf die **WMI zurückgreifen**, sollten hier gleich die korrekten Berechtigungen berücksichtigt werden.

Öffnen Sie dazu die **Computerverwaltung** auf dem System (**compmgmt.msc**). Unter dem Punkt **„Lokale Benutzer und Gruppen**“ wählen Sie unter **Gruppen** die **Eigenschaften** von „**Leistungsprotokollbenutzer**„.

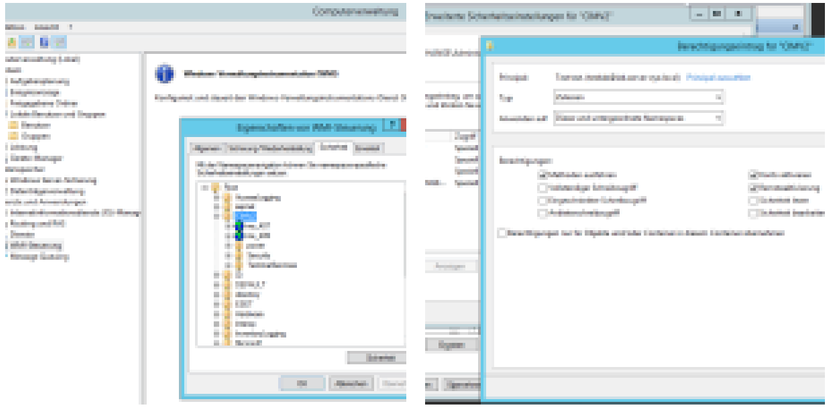


Fügen Sie hier ihren Benutzer hinzu um die Berechtigung zu setzen.



Danach ist es notwendig unter **WMI-Steuerung die Dienste und Anwendungen** anzupassen. Folgendes Element interessiert uns, **CIMV2.** Gegebenfalls kann es **je nach Anwendungszweck notwendig sein auch bei anderen Namespaces Berechtigungen**

durchzuführen. Die notwendigen Einstellungen finden Sie auf CIMV2 unter dem Punkt **Sicherheit –>Erweitert.**



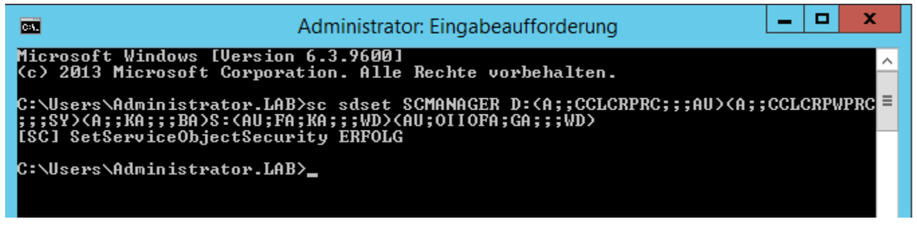
Danach fügen Sie den gewollten Benutzer hinzu mit den aufgeführten Berechtigungen „**Methoden ausführen**„, „**Konto aktivieren**„, „**Remoteaktivierung**“ und unter Anwenden auf „**Dieser und untergeordnete Namespaces**“

Ergänzend dazu finden Sie eine Dokumentation auch hier in der MSDN.

Schritt 4 – Dienstberechtigungen setzen

Zuletzt müssen Sie noch sicherstellen, dass wir auf die **Diensteverwaltung** zugreifen dürfen. Dies geht mittels folgendem Befehl in einer **als Administrator gestarteten Eingabeaufforderung** (Cmd.exe):

- *sc sdset SCMANAGER D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)*



Diese Information basiert auf einem KB Artikel von Microsoft.

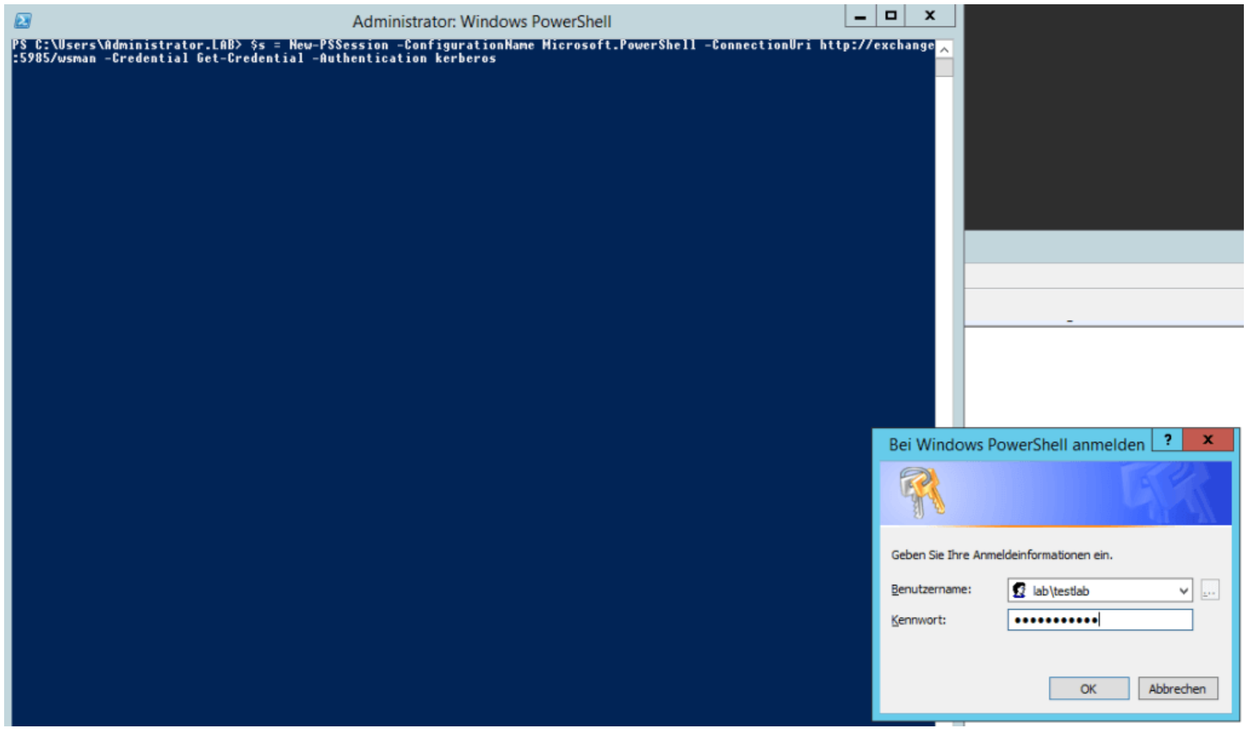
Schritt 5 – Testlauf

Abschließend sollten wir einmal kurz testen ob alles erfolgreich angewandt wurde.

Dazu öffnen wir die **PowerShell** und führen folgenden **Befehlsablauf** durch:

- $mySession = New-PSSession -ConfigurationName Microsoft.PowerShell -ConnectionUri http://DerServerNameNichtDieIP:5985/wsman -Credential Get-Credential -Authentication kerberos

Anschließend geben Sie die **Zugangsdaten** des Benutzers ein.



Wenn der Befehl erfolgreich war, sollten Sie dies an einer **Änderung der Shell** sehen können. Im Fall dieses Beispiels haben wir eine Verbindung zum **Exchange Server** aufgebaut.

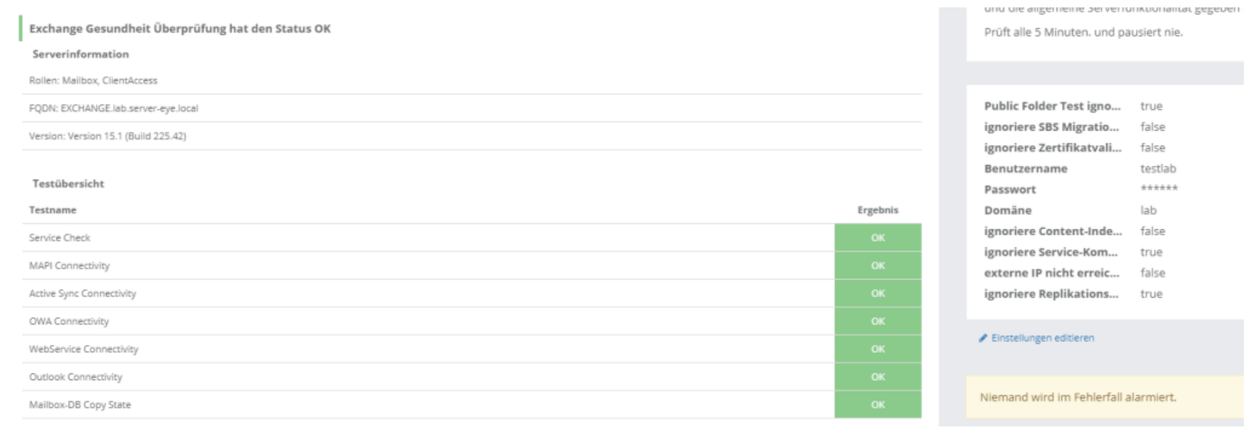
Als nächstes können wir zum Testen noch den Befehl *Get-WmiObject Win32_Service |FT* eingeben**.**

Dadurch haben wir zum einen den **WMI Zugriff** als auch den **Dienstkonto-Zugriff durchgetestet**.

```
[exchange]: PS C:\Users\testlab\Documents>
[exchange]: PS C:\Users\testlab\Documents> Get-WmiObject Win32_Service |FT

ExitCode Name                      ProcessId StartMode State   Status
-------- ----                      --------- --------- -----   ------
    1077 AppMgmt                           0 Manual    Stopped OK
       0 BrokerInfrastruc...             548 Auto      Running OK
       0 DcomLaunch                      548 Auto      Running OK
       0 Dhcp                            688 Auto      Running OK
       0 Dnscache                        900 Auto      Running OK
    1077 EFS                               0 Unknown   Stopped UNKNOWN
       0 EventLog                        688 Auto      Running OK
```

Infolge dessen können wir nun ins **OCC wechseln** und unseren Exchange Gesundheit Sensor mit dem erstellten Benutzer testen.



Unter dem Strich müssen wir also einiges tun um die korrekten Berechtigungen zu setzen. Entscheiden Sie selbst, was für Sie die richtige Vorgehensweise ist ☺

Wir freuen uns über eine Bewertung!

★★★★★

Entwicklung, Hosting und Support erfolgen zu 100% in Deutschland.

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Hier können Sie sich die Datei herunterladen: