PSMail – Server-Statusreport

RB-Tool zum Versenden eines einfachen Statusreport

Vorarlberger Standardschulinstallation
Autor: Lukas Franz
Besuchen Sie uns im Internet
http://www.vobs.at/rb

1. Inhalt

2. Vorbemerkung

Mit dem PowerShell-Skript RB-PSMail_ServerStatusRep_v4.0.ps1 kann zusammen mit dem PS-MAIL30-Skript ein kleiner Statusreport vom Server einer Schule gesendet werden.

Der Bericht wird direkt in ein Mail geschrieben und beinhaltet:

- Freier Speicher auf den wichtigsten Laufwerken von Server und DCSchule
- Status des Dienstes WSUS
- Status des Dienstes WDS
- Status des Dienstes ADSync
- Größe des WSUS-Content-Ordners und der Datei SUSDB.mdf
- Eventuell verfügbare Softwareupdates

Das Skript wird wie jedes PowerShell-Skript per Task in der Aufgabenplanung aufgerufen.
Es muss nach den eigenen Anforderungen angepasst werden.

In den bisherigen Versionen des Skripts wurde das Ganze vom Host1 aus aufgerufen. Davon sind wir aus unterschiedlichen Gründen abgekommen. Es geht hierbei in erster Linie um Zugriffsrechte vom host1 aus auf die Domäne Schule bzw. auf die VMs Server und DCSchule.
Zu verschmerzen dürfte sein, dass somit der Replikationsstatus, der Speicherplatz auf Host1 und der Status der virtuellen Maschinen nicht im Bericht vorkommt. Wir werden dafür in absehbarer Zeit ein eigenes Tool nachreichen.

3. ToDo

Entpacken der Datei RB-PSMail_ServerStatusReport_v4.0.ps1 auf dem Server nach \\schule.aps\dfs\Setup$_Administrator\RB-PSMail\RB-ServerStatusReport.

Im Skript an sich ist der Pfad zum **PS-Mail-Skript** in Zeile 9 anzupassen:

```
1  #Dieses Skript funktioniert nur zusammen mit dem Email-Skript PSMail30
2
3  #Variable
4  #Namen der Virtuellen Maschinen eintragen
5  $Datum = Get-Date
6  $Sender = $env:COMPUTERNAME
7  $DC = "DCSchule"
8  $SRV = "Server"
9  $PSMAILPATH = "\\schule.aps\dfs\Setup$\_Administrator\RB-PSMail\RB-PSMail"
10
11 # Freier Speicher auf Server, DC und host1 auslesen
12 $SRVC1 = Get-WmiObject win32_logicaldisk -Computer $SRV -filter "name='c:'" | select
13 $SRVC2 = $SRVC1.freespace
14 $SRVC = [math]::Round($SRVC2/1GB,2)
15
16 $SRVD1 = Get-WmiObject win32_logicaldisk -Computer $SRV -filter "name='d:'" | select
17 $SRVD2 = $SRVD1.freespace
18 $SRVD = [math]::Round($SRVD2/1GB,2)
```

Erstellen eines Tasks im Taskplaner:

Ausführen unabhängig von der Benutzeranmeldung als Domänen-Administrator.
Trigger beliebig. Z.B. täglich um 6.00 Uhr.
Aktion – Programm starten

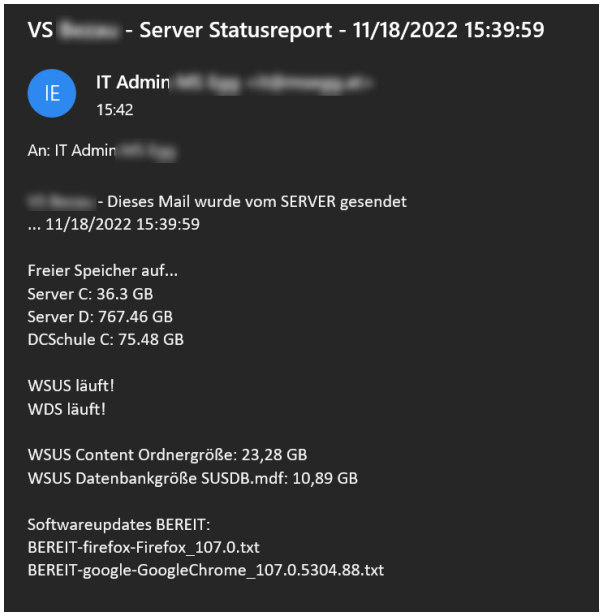
Programm/Script: *C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe*
Argumente: *-ExecutionPolicy Bypass "\\schule.aps\dfs\Setup$_Administrator\RB-PSMail\RB-ServerStatusReport\RB-PSMail_ServerStatusRep_v4.0.ps1"*

Alternativ kann der Task auch über die im Paket enthaltene Datei Task_RB-ServerStatusReport.xml importiert werden. Pfade und Einstellungen müssen entsprechend kontrolliert bzw. angepasst werden.

HINWEIS zum Dienst ADSync: Ist an einer Schule die AD-Verzeichnissynchronisation gar nicht eingerichtet, erscheint beim Testdurchlauf des Skripts eine Fehlermeldung. Das Info-Mail wird jedoch trotzdem versendet und die Zeile über den Status des ADSync-Dienstes erschient gar nicht.

4. Ergebnis

Ist RB-PSMail richtig konfiguriert, wird ein Mail mit entsprechendem Inhalt versendet:



5. Skript-Inhalt

```
#Dieses Skript funktioniert nur zusammen mit dem Email-Skript PSMail30

#Variable
#Namen der Virtuellen Maschinen eintragen
$Datum = Get-Date
$Sender = $env:COMPUTERNAME
$DC = "DCSchule"
$SRV = "Server"
$PSMAILPATH = "\\schule.aps\dfs\Setup$\_Administrator\RB-PSMail\RB-PSMail"

# Freier Speicher auf Server, DC und host1 auslesen
$SRVC1 = Get-WmiObject win32_logicaldisk -Computer $SRV -filter "name='c:'" | select name, volumename, freespace
$SRVC2 = $SRVC1.freespace
$SRVC = [math]::Round($SRVC2/1GB,2)

$SRVD1 = Get-WmiObject win32_logicaldisk -Computer $SRV -filter "name='d:'" | select name, volumename, freespace
$SRVD2 = $SRVD1.freespace
$SRVD = [math]::Round($SRVD2/1GB,2)

$DCC1 = Get-WmiObject win32_logicaldisk -Computer $DC -filter "name='c:'" | select name, volumename, freespace
$DCC2 = $DCC1.freespace
$DCC = [math]::Round($DCC2/1GB,2)

$Body2 = "Freier Speicher auf... <br>$SRV C: $SRVC GB <br>$SRV D: $SRVD GB <br>$DC C: $DCC GB <br>"

#WSUS läuft
$wsus = get-service *wsusser* -computername $SRV
if($wsus.status -eq "Running")
    {$WSUSStatus="WSUS läuft!"}
    else
    {$WSUSStatus="WSUS läuft NICHT!!"}

#WDS läuft
$wds = get-service WDSServer -computername $SRV
if($wds.status -eq "Running")
    {$WDSStatus="WDS läuft!"}
    else
    {$WDSStatus="WDS läuft NICHT!!"}

#ADSync läuft
$adsync = get-service ADSync -computername $SRV
if($adsync.status -eq "Running")
    {$ADSyncStatus="ADSync läuft!"}
    else
    {$ADSyncStatus="WDS läuft NICHT!!"}
```

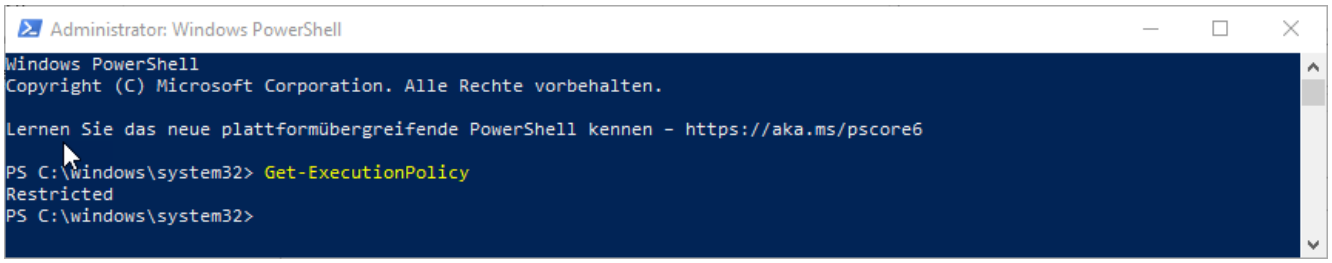
```
#Body für Dienste-Status zusammensetzen
$Body3 = "$WSUSStatus<br>$WDSStatus<br>$ADSyncStatus"

#WSUS Größe Datenbank und Contentordner
$WSUSCont = (Get-ChildItem -Path \\server\CDs$\WSUS\WsusContent -Force -Recurse -ErrorAction SilentlyContinue |
Measure-Object -Property Length -Sum).Sum
$WSUSDB = (get-childitem \\server\c$\Windows\WID\Data\SUSDB.mdf | select-object length).length

$Body4 = 'WSUS Content Ordnergröße: {0:n2} GB' -f ($WSUSCont/1GB)
$Body5 = 'WSUS Datenbankgröße SUSDB.mdf: {0:n2} GB' -f ($WSUSDB/1GB)

#Softwareupdates bereit
$SWUP = ((Get-ChildItem \\server\Softwareverteilung\_autodownload\BEREIT*.*).Name -join "<br>")
if ($SWUP -eq $null)
    {$Body6 = "KEINE Softwareupdates BEREIT!"}
    else
    {$Body6 = "Softwareupdates BEREIT:<br>$SWUP"}


#Email Body zusammenfügen
$Body0 = "Dieses Mail wurde vom $Sender gesendet <br>... $Datum<br>"
$Body = "$Body0<br>$Body2<br>$Body3<br><br>$Body4<br>$Body5<br><br>$Body6"

#Email senden
Push-Location $PSMAILPATH
.\PSMail30.ps1 -EmailSubject "Server Statusreport - $Datum" -EmailBody $Body
```

6. Anhang

6.1. Problemlösungen bei Problemen beim Mailversand

Powershell Befehle zulassen (bei Bedarf)

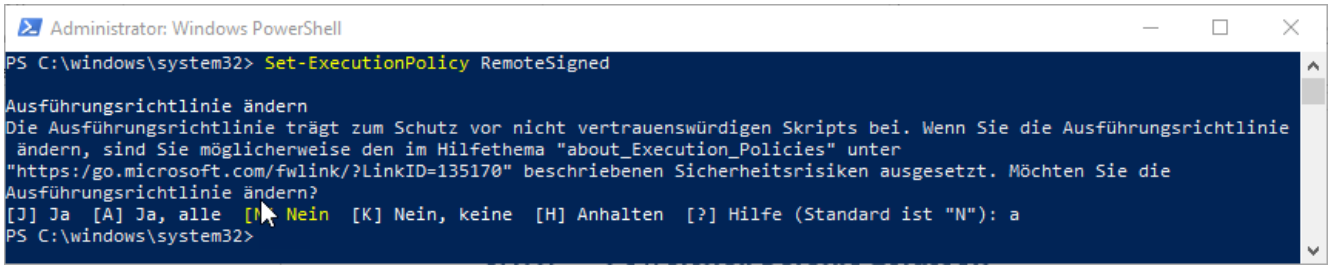
```
Get-ExecutionPolicy
```



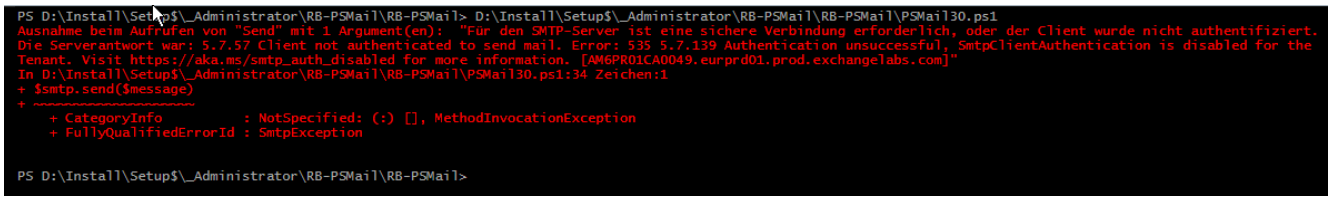
Ist das Ergebnis „Restricted“

```
Set-ExecutionPolicy RemoteSigned
```

„a“ für alle



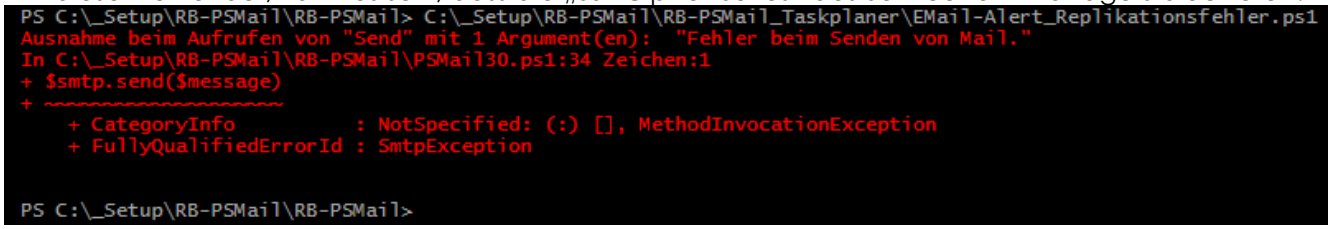
SMTP-Versand ermöglichen (bei Bedarf)



Für den Versand von Mails muss zwingend der SMTP-Versand für die M365-Mailadresse am Tenant erlaubt werden.
Siehe Microsoft-365-SMTP-Authentication_v22.x.pdf

Fehler beim Mailversand

Tritt dieser Fehler auf, kann es sein, dass die „SSL Cipher-Suites“ des ServicePointManagers blockieren.



Lösung: „Freigabe“ der Ciphers im Skript

- nur für die verwendeten Ciphers (Tls12 reicht vermutlich aus)

```
[System.Net.ServicePointManager]::SecurityProtocol = 'Tls,Tls11,Tls12'
```

• alle Ciphers

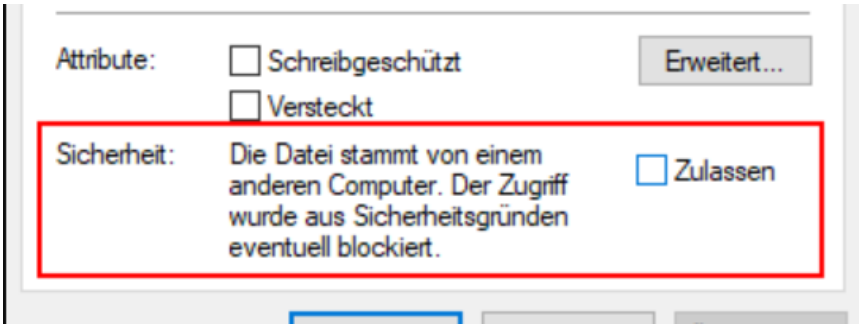
```
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.SecurityProtocolType]::GetNames([System.Net.SecurityProtocolType])
```

Ergänzung in **PsMail30.ps1** NUR BEI BEDARF

```
#Definition der Parameter, welche übergeben werden

Param(
[string]$EmailSubject,
[string]$EmailBody,
[string]$File
) [

System.Net.ServicePointManager]::SecurityProtocol = 'Tls12'

#Variable aus config.ini importieren
$config = get-content .\config.ini
…
```

Mailversand funktioniert „händisch", nicht aber im Taskplaner

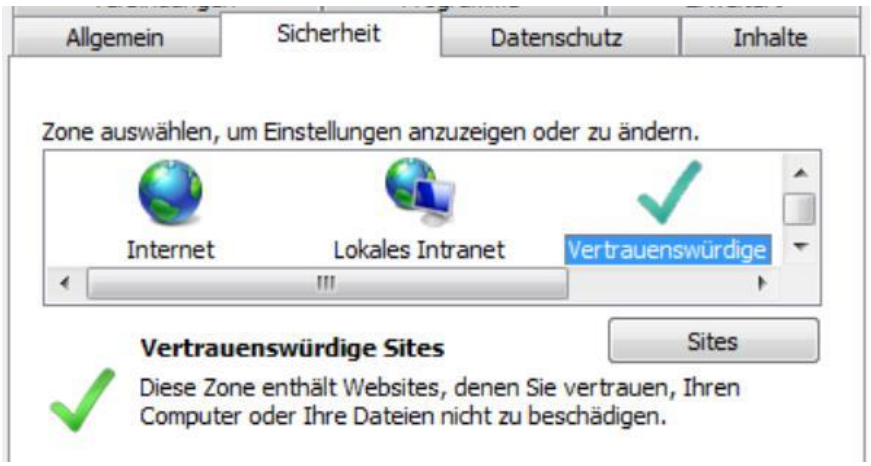
Das Blockieren des Ausführens von Dateien aufheben
Werden nach dem Download einer ZIP-Datei die Eigenschaften dieser angezeigt, so erschient möglicherweise ein Block „Sicherheit" mit folgendem Hinweis: „Die Datei stammt von einem anderen Computer. Der Zugriff wurde aus Sicherheitsgründen eventuell blockiert."



Ein Klick auf „Zulassen" lässt diese Sicherheitswarnung verschwinden. Macht man das nicht, wirkt es sich auf alle im ZIP-File enthaltenen ausführbaren Dateien aus.

Hier würde das bedeuten, dass die PSMail-PowerShell-Skripts nicht ausgeführt werden können, wenn sie im Taskplaner eingebaut sind. Und genau das ist bei den meisten ja vorgesehen.

Eine andere Möglichkeit, das Setzen dieses Sicherheits-Attributs vorab zu unterbinden ist, die Downloadseite https://www.vobs.at den Vertrauenswürdigen Sites in den Internetoptionen hinzuzufügen:
Systemsteuerung – Internetoptionen - Sicherheit.

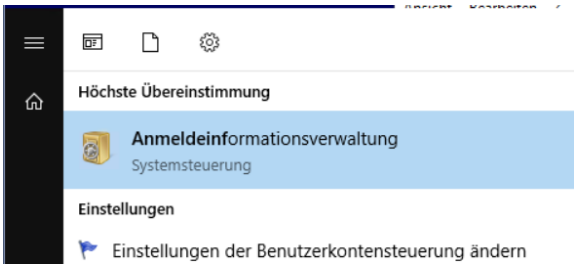


Über Sites können URLs hinzugefügt werden, bei denen am Ende eines Downloads keine Sicherheitsüberprüfung ausgeführt wird. Damit entfällt für alle vom VOBS heruntergeladenen Dateien der oben beschriebene Klick auf „Zulassen“.

Dies ist unabhängig davon, ob Dateien über Internetexplorer oder Chrome heruntergeladen werden.

6.2. Zugriffsdaten auf dem Host1 wieder entfernen

Die gespeicherten Zugriffsdaten sind in der *Anmeldinformationsverwaltung* bei *Windows-Anmeldeinformationen* zu finden.



Dort können die entsprechenden Einträge entfernt werden.