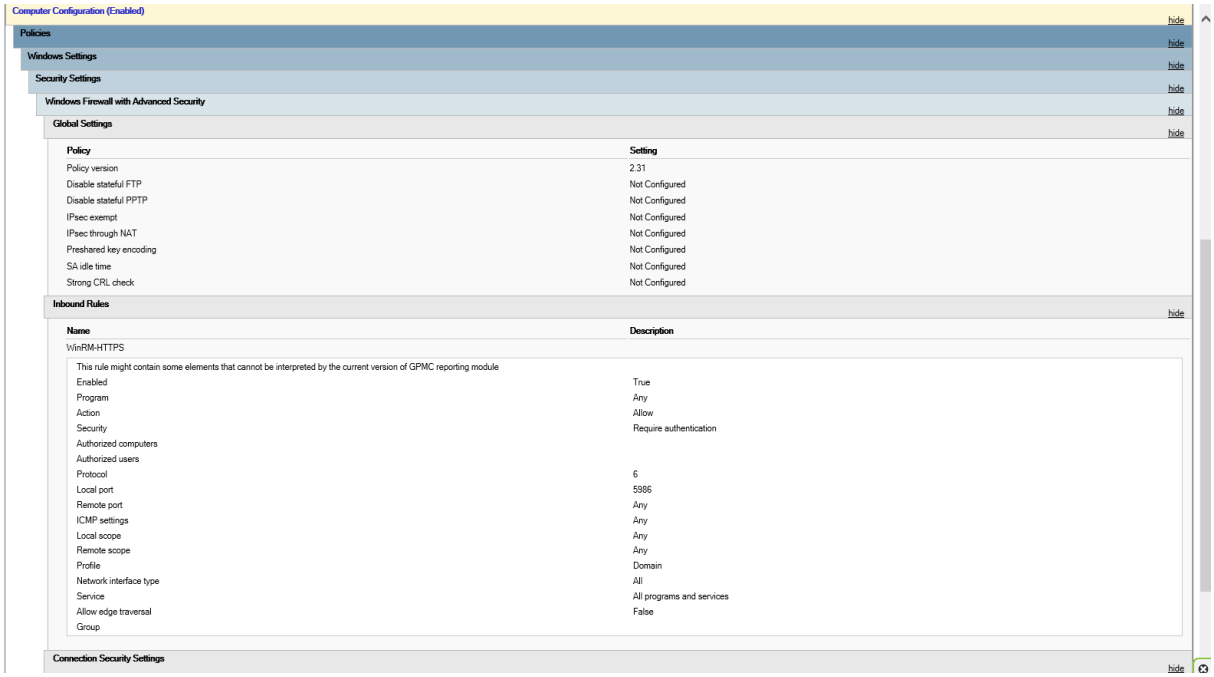
WinRM-CertAuth

Für das automatische Deployment von Zertifikaten und den zu setzenden Einstellungen zur Absicherung von WinRM, ist folgendes zu tun.

GPO

Das neue Gruppenrichtlinienobjekt benötigt eine Richtlinie zur Freischaltung des lokalen eingehenden Ports 5986 und zwar nur für das Domänenprofil.



Computer Configuration (Enabled) hide
Policies hide
Windows Settings hide
Security Settings hide
Windows Firewall with Advanced Security hide
Global Settings hide

Policy	Setting
Policy version	2.31
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Inbound Rules hide

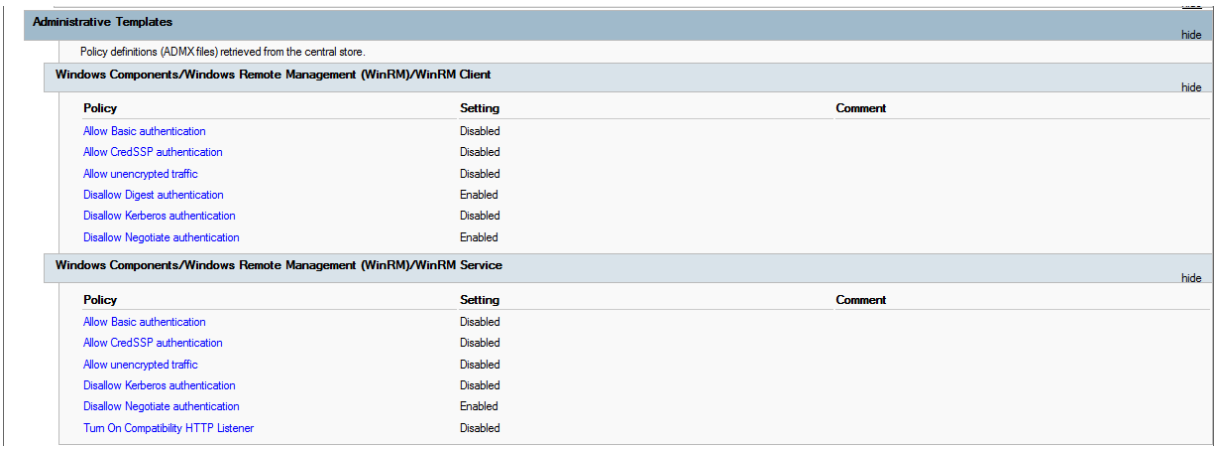
Name	Description
WinRM-HTTPS	

This rule might contain some elements that cannot be interpreted by the current version of GPMC reporting module

Enabled	True
Program	Any
Action	Allow
Security	Require authentication
Authorized computers	
Authorized users	
Protocol	6
Local port	5986
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	Any
Profile	Domain
Network interface type	All
Service	All programs and services
Allow edge traversal	False
Group	

Connection Security Settings hide

Die Windows Remote Management-Einstellungen sollten für Client/Server wie folgt aussehen. * Negotiate wird gebraucht *



Administrative Templates hide

Policy definitions (ADMX files) retrieved from the central store.

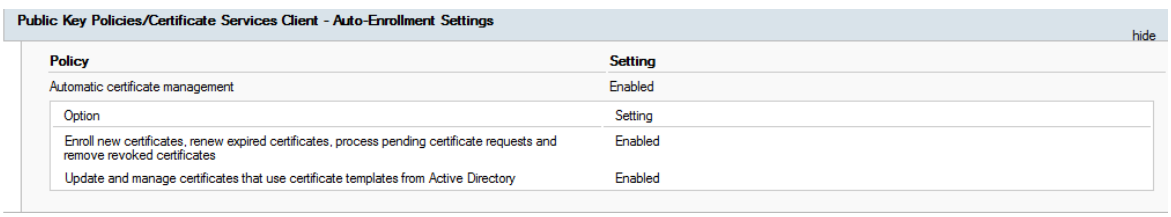
Windows Components/Windows Remote Management (WinRM)/WinRM Client hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow CredSSP authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow Digest authentication	Enabled	
Disallow Kerberos authentication	Disabled	
Disallow Negotiate authentication	Enabled	

Windows Components/Windows Remote Management (WinRM)/WinRM Service hide

Policy	Setting	Comment
Allow Basic authentication	Disabled	
Allow CredSSP authentication	Disabled	
Allow unencrypted traffic	Disabled	
Disallow Kerberos authentication	Disabled	
Disallow Negotiate authentication	Enabled	
Turn On Compatibility HTTP Listener	Disabled	

Das automatische Enrollment muss folgende Einstellungen gesetzt bekommen!



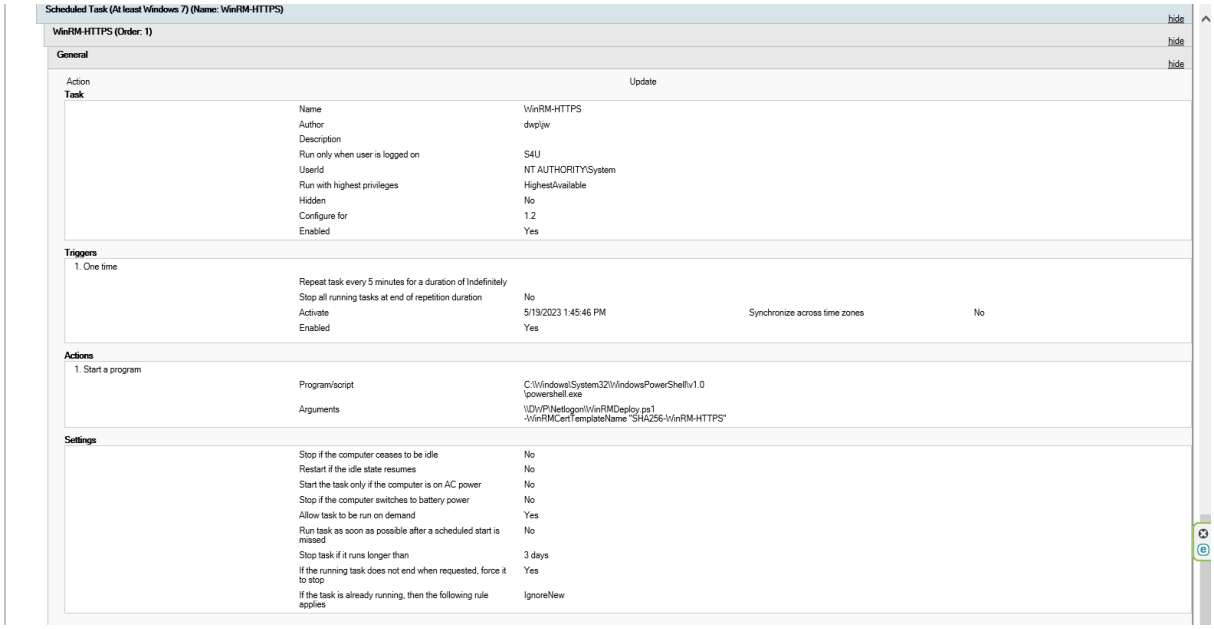
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings hide

Policy	Setting
Automatic certificate management	Enabled

Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

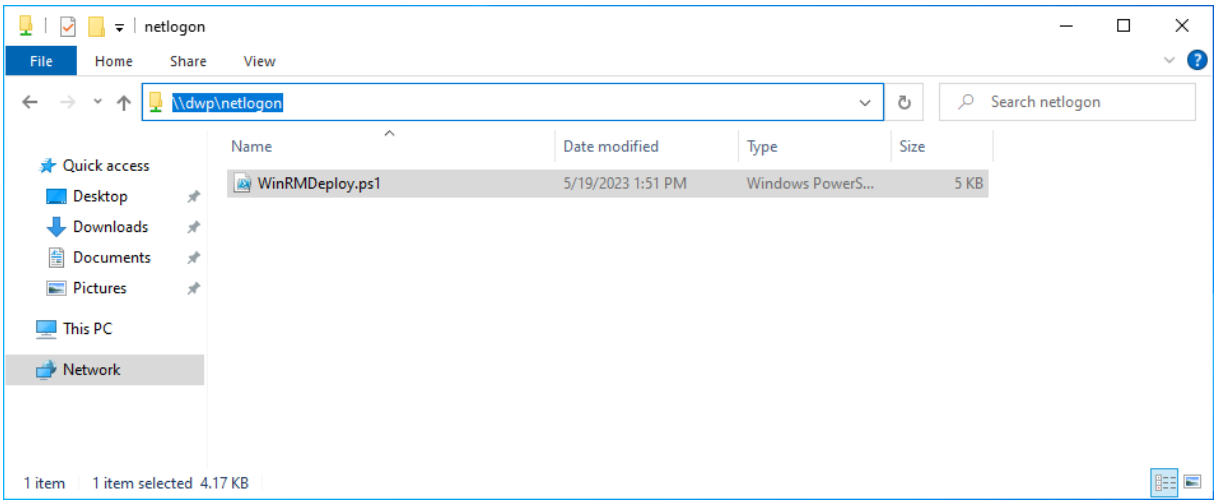
Erstellt von Jörn Walter **19.05.2023**

Der Scheduled-Task braucht keine besonderen Parameter zum Starten des Skripts. Es sollte jedoch signiert sein, um in keine andere (Powershell-signierte Skripte) Härtungsfalle zu laufen.



Netlogon:

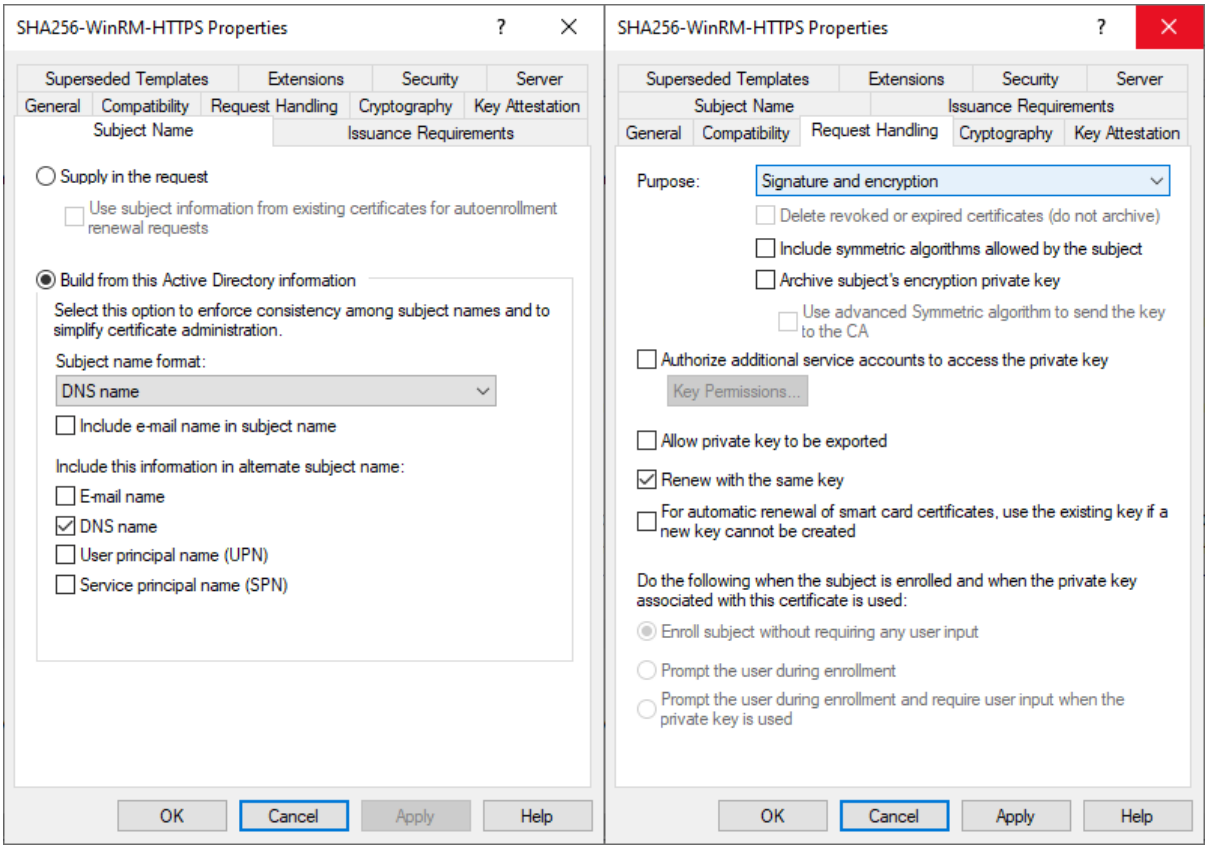
Für die Skript-Freigabe reicht die Gruppe der Authenticated Users aus.



WinRM-CertAuth

Certificate Authority:

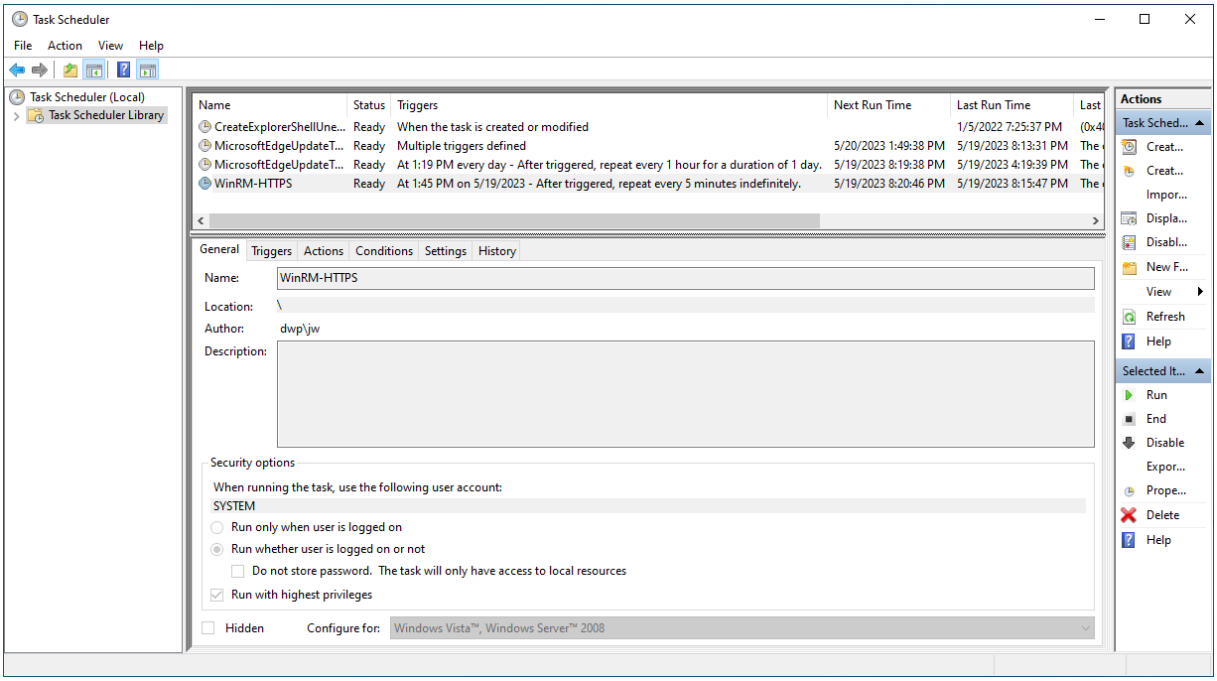
Das Certificate-Template benötigt lediglich die im Bild zu sehenden Settings. Im Format entweder DNS name oder Common Name.



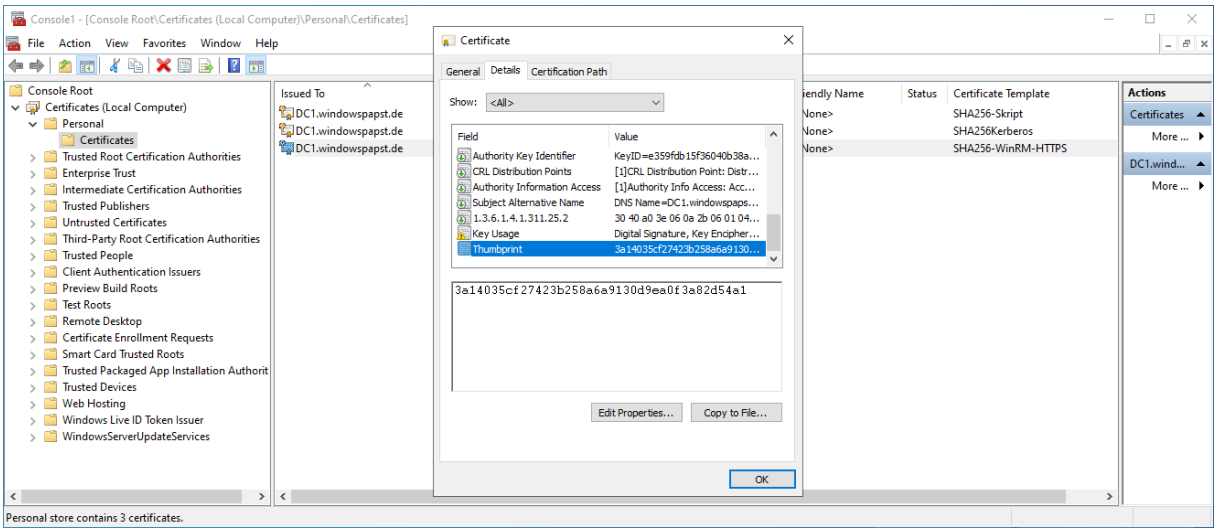
Deployment:

Nachdem das GPO angewendet wurde, sollte der Task auf dem Member-Server in der Library zu sehen sein.

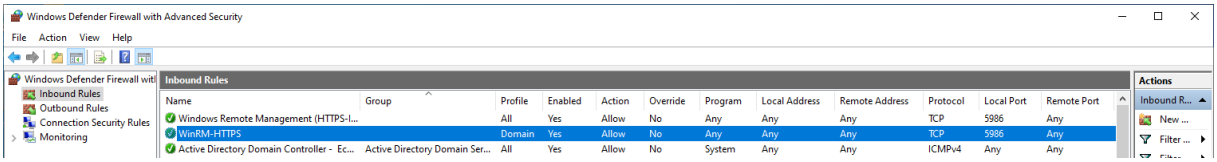
WinRM-CertAuth



Das Zertifikat sollte ebenfalls schon vorhanden sein. Wenn nicht, dann wird das gesteuerte Skript nochmals ein gpupdate ausführen, um den Prozess anzustoßen. Andernfalls per certutil -pulse; sollte aber nicht nötig sein.

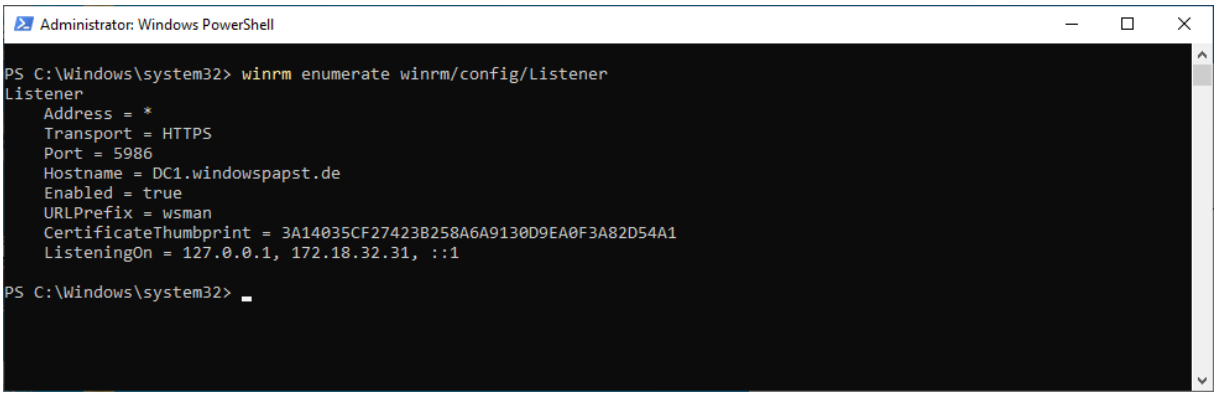


Auf dem Member-Server sollte ebenfalls der eingehende Firewallport 5986 freigeschaltet sein.

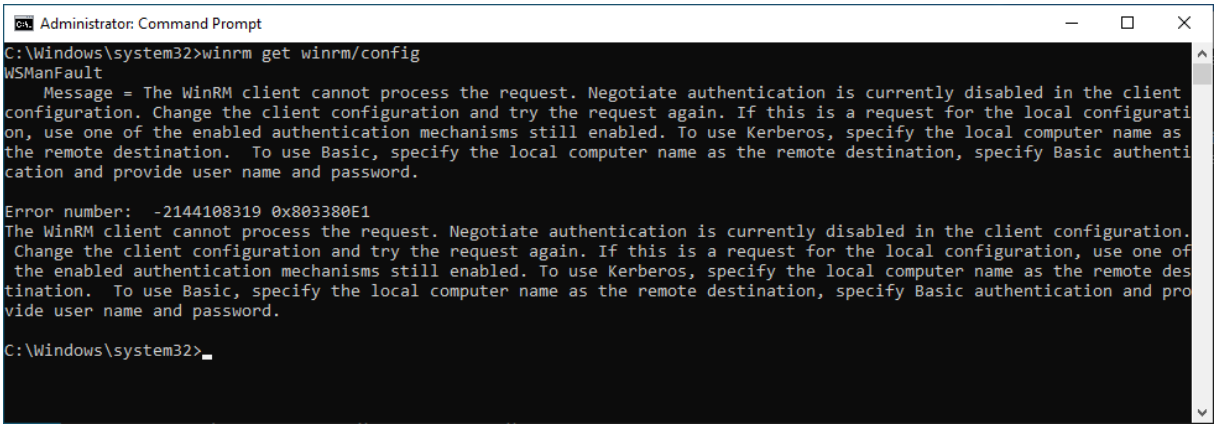


Erstellt von Jörn Walter **19.05.2023**

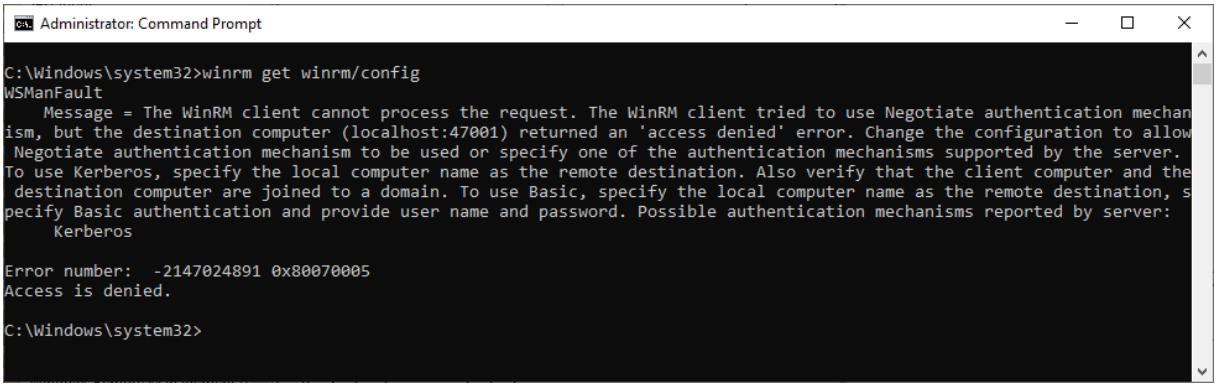
Zur Kontrolle fragen wir die WinRM-Listener ab. Das neue Zertifikat sollte gebunden sein. Kontrolle des Thumbprints.



Die Member-Server WinRM-Config sollte alle Policy-Einstellungen aus dem GPO wiedergeben. Leider funktioniert die Abfrage nicht ohne Negotiate.

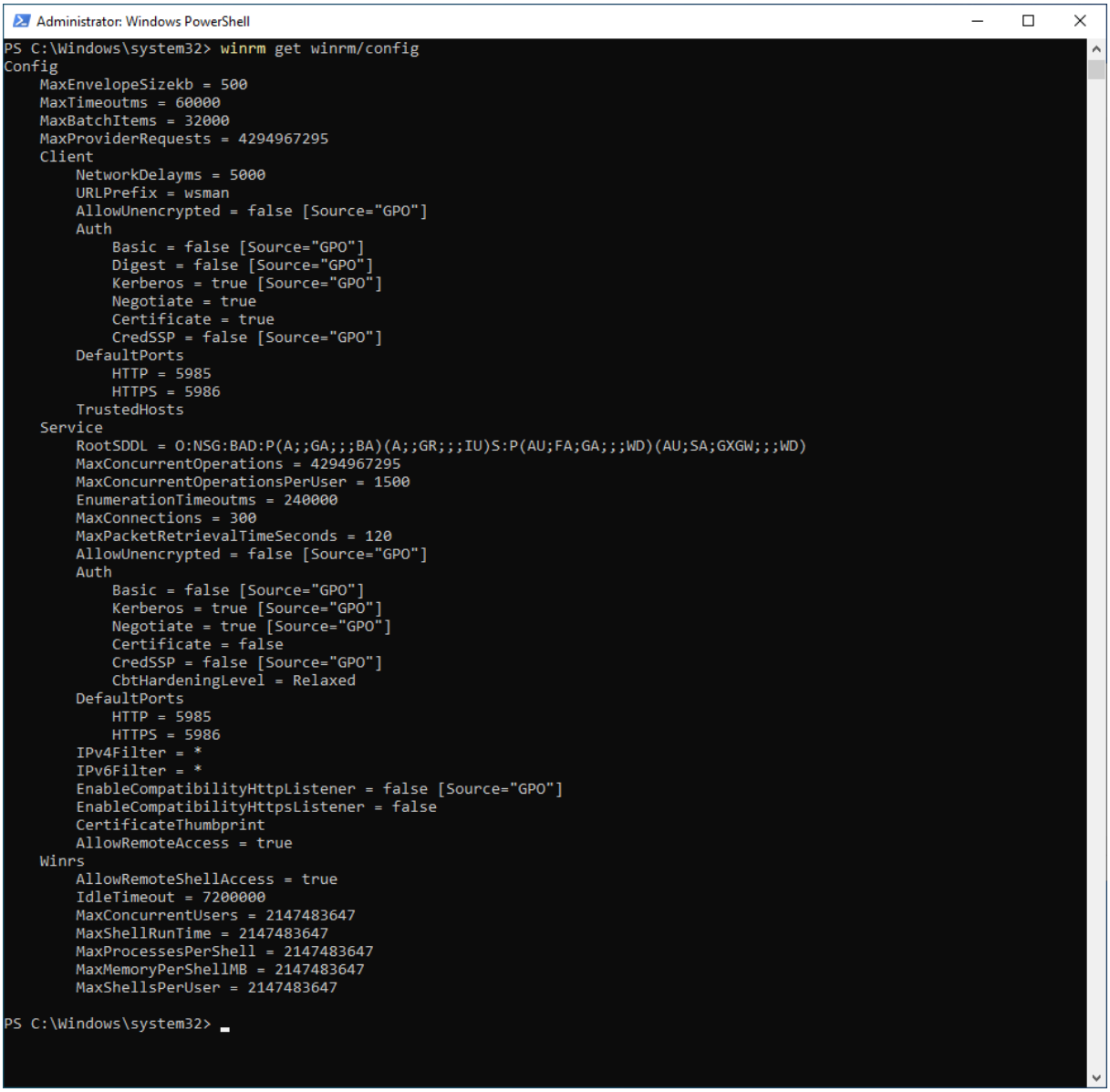


Wenn Negotiate nur Client-seitig aktiv ist erscheint folgende Ausgabe:



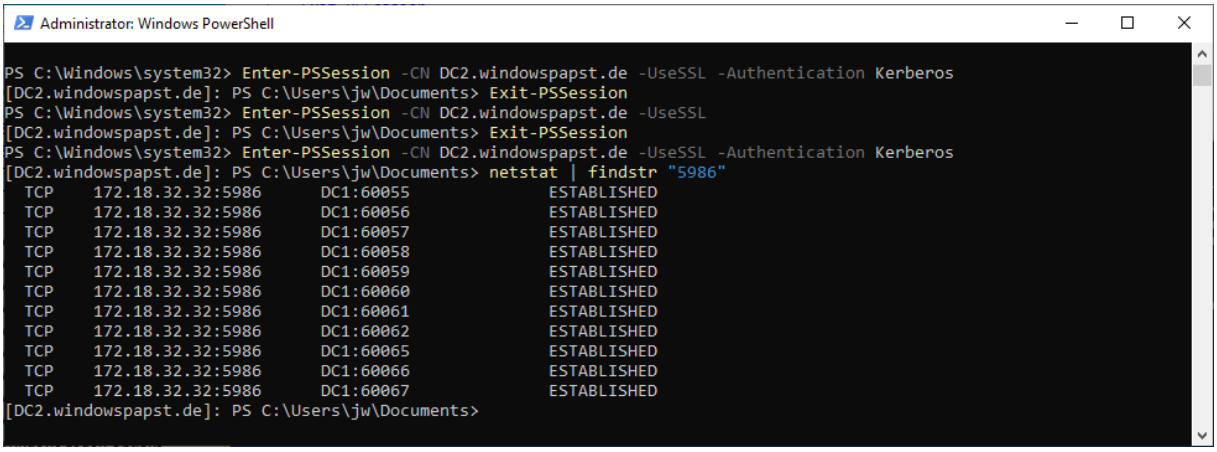
WinRM-CertAuth

Sobald der Authentifizierungsmechanismus Negotiate Client/Server-seitig wieder zur Verfügung steht, kann auch die Konfiguration wieder abgefragt werden. Nur interessant sofern es abgeschaltet wurde.

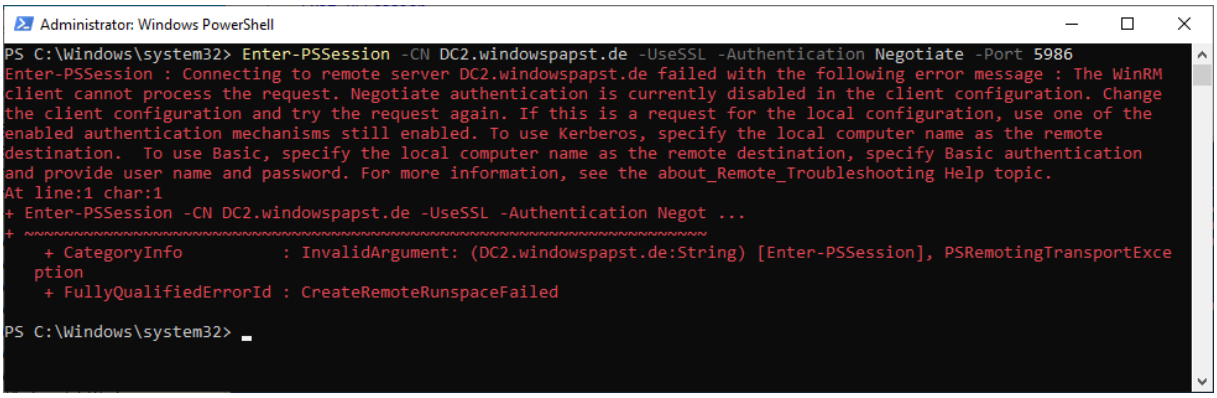


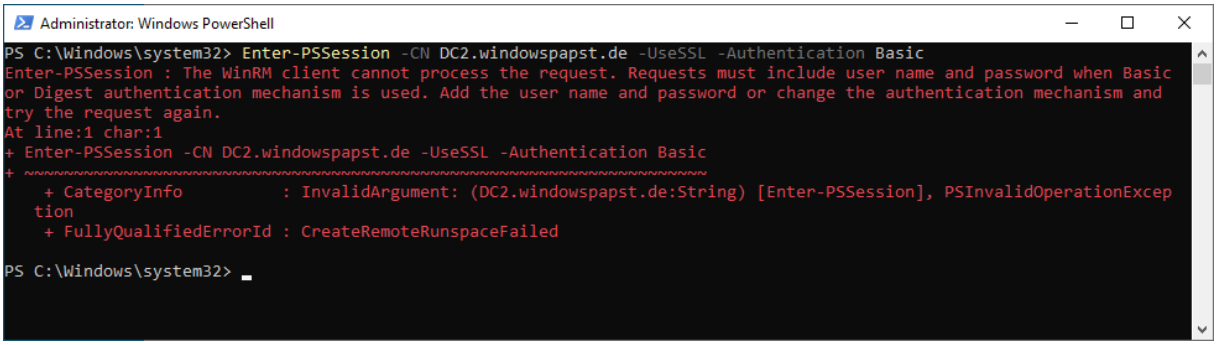
WinRM-CertAuth

Member-Server Connection-Test via SSL & Kerberos:



Der Versuch über Negotiate und Basic Auth ist gescheitert sofern deaktiviert!





Problem!

Negotiate wird für den automatischen Task und für weitere Aufgaben benötigt. Ohne Negotiate gibt es auch Probleme mit dem Server Manager.

WinRM-CertAuth

Authentication-Methods

Es gibt 3 Möglichkeiten der Authentifizierung.

1: Basisauthentifizierung

Auf dem Zielsystem erfolgt die Anmeldung über einen lokalen Benutzer. Passwort und Daten werden unverschlüsselt (Base64 ist keine Verschlüsselung) per HTTP übertragen.

2: Domänenbenutzerauthentifizierung

Die Authentifizierung erfolgt über Kerberos. Die Übertragung der Nutzerdaten erfolgt weiterhin unverschlüsselt per HTTP.

- Der Benutzer muss Mitglied der lokalen Administratoren sein.
- Die WinRM-Config wird erwartet: Auth Kerberos = true; Auth Basis=false; AllowUnencrypted=false

3: Zertifikatbasierte Authentifizierung

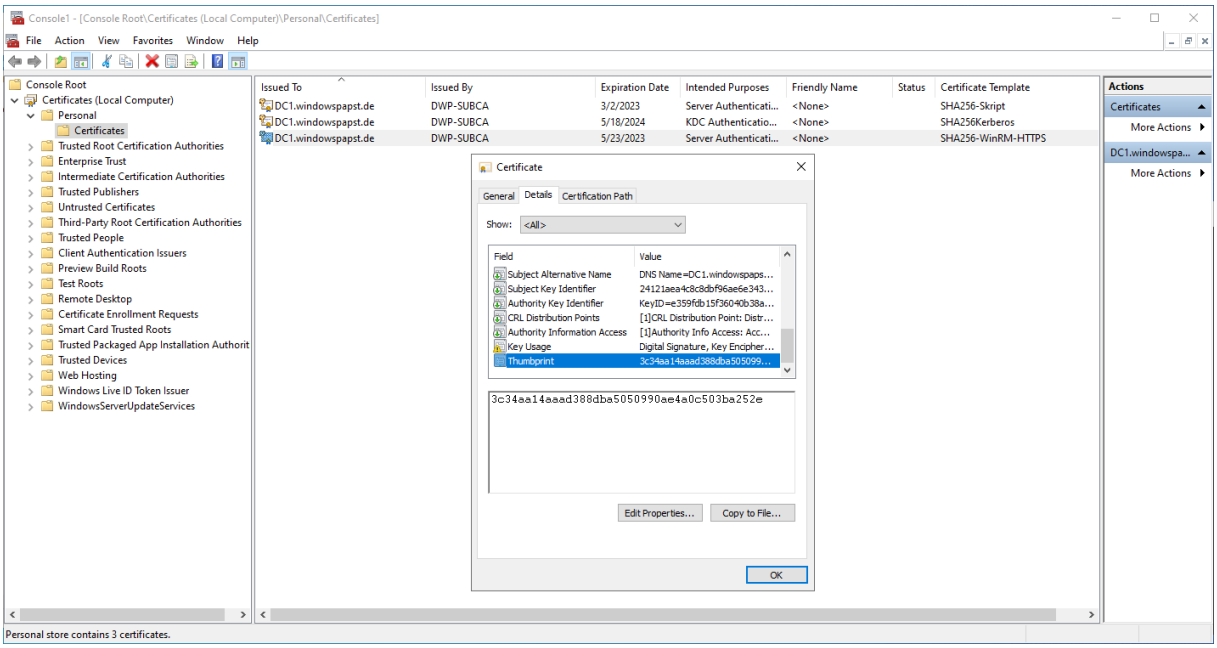
Voraussetzung ist, dass das Zielsystem über ein eigenes Serverzertifikat verfügt. In diesem Fall werden sowohl die Anmeldung als auch die Daten verschlüsselt über HTTPS übertragen.

- SHA-256 Zertifikat
- WinRM HTTPS-Listener
- Funktionierende Kerberos Authentifizierung

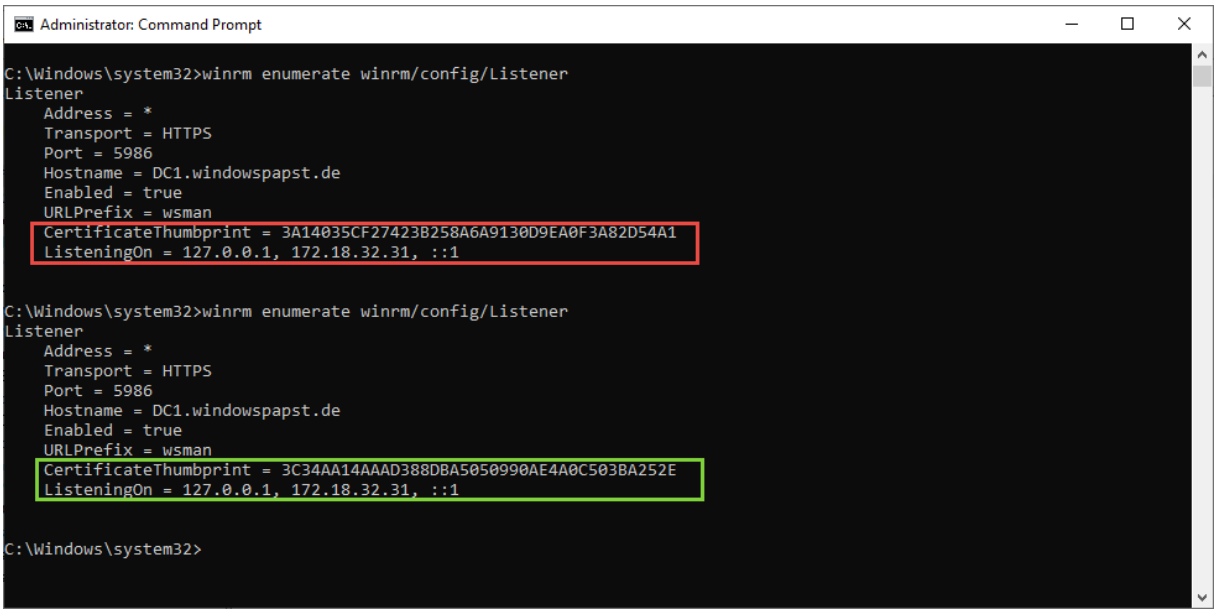
WinRM-CertAuth

Certificate Renewal Process

Das Zertifikat wurde während der Renewal Phase automatisch erneuert.



Der Deployment Task hat erkannt, dass das alte und bereits ersetzte Zertifikat nicht mehr der ursprünglichen Konfiguration entspricht und hat es somit an das aktuelle Zertifikat gebunden.

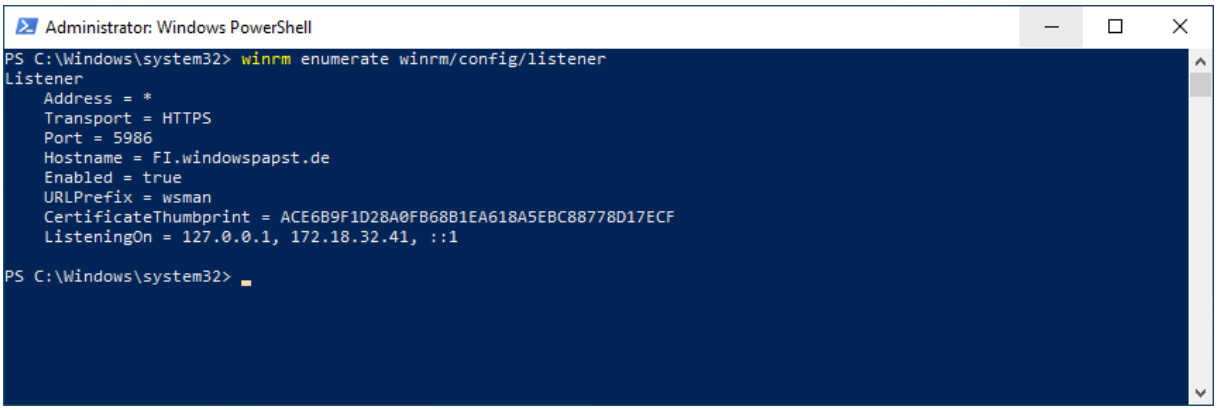


WinRM-CertAuth

Remove HTTPS-Config and Re-Create http Listener

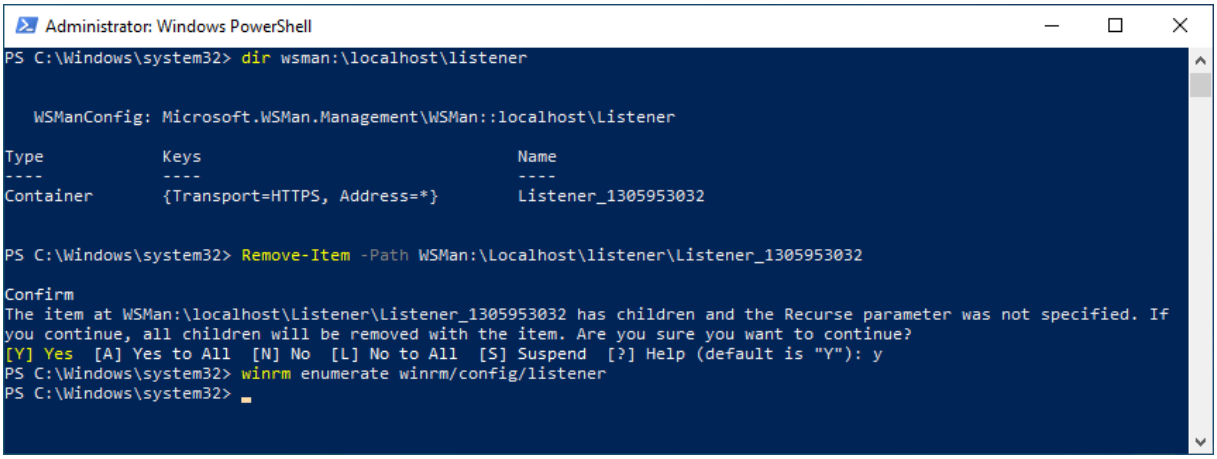
Zuerst geben wir die Listener samt Thumbprints aus. Das dient lediglich der Überprüfung.

winrm enumerate winrm/config/listener



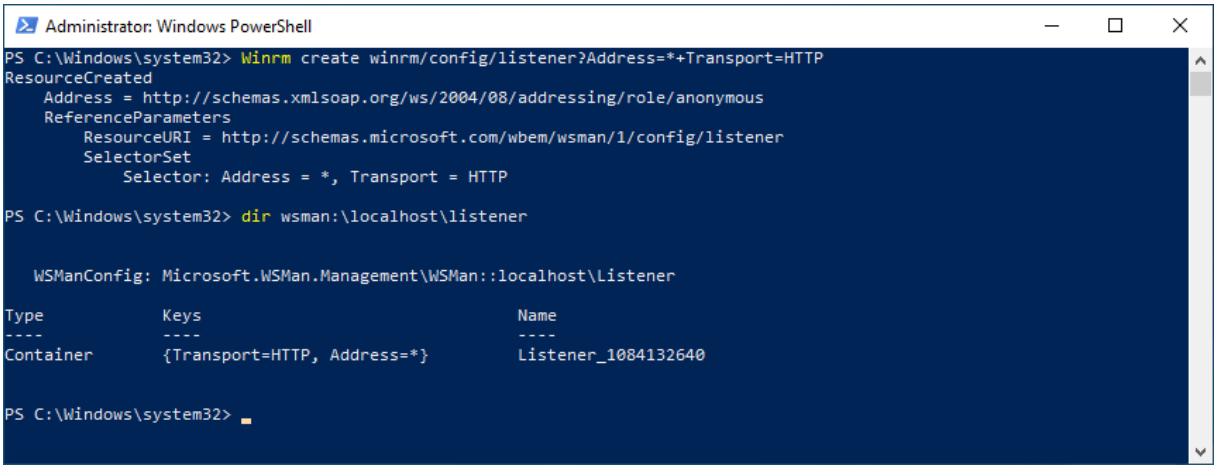
Als nächstes liest man den/die Listener-ID aus und löscht diese anschließend.

dir wsman:\localhost\listener
Remove-Item -Path WSMan:\Localhost\listener\Listener_1305953032



Zum Abschluss stellt man den http Listener wieder her.

Winrm create winrm/config/listener?Address=*+Transport=HTTP
dir wsman:\localhost\listener



Erstellt von Jörn Walter **19.05.2023**

WinRM-CertAuth

Manuelle Umsetzungshilfe – Cert-Binding:

New-SelfSignedCertificate –DnsName ([System.Net.Dns]::GetHostByName($env:computerName)).Hostname -CertStoreLocation "cert:LocalMachineMy" -FriendlyName DC1

$thumb = Get-ChildItem Cert:LocalMachineMy | where FriendlyName -eq DC1 | select Thumbprint

New-WSManInstance -ResourceURI winrm/config/Listener -SelectorSet @{address="*";transport="https"} -ValueSet @{Hostname=[System.Net.Dns]::GetHostByName(($env:computerName)).Hostname;CertificateThumbprint=$dump.thumbprint

winrm e winrm/config/listener

winrm set winrm/config/service/auth @{Certificate="true"}

Das beiliegende Powershell-Skript habe ich so gestaltet, das es für englische und deutsche Systeme geeignet ist.