

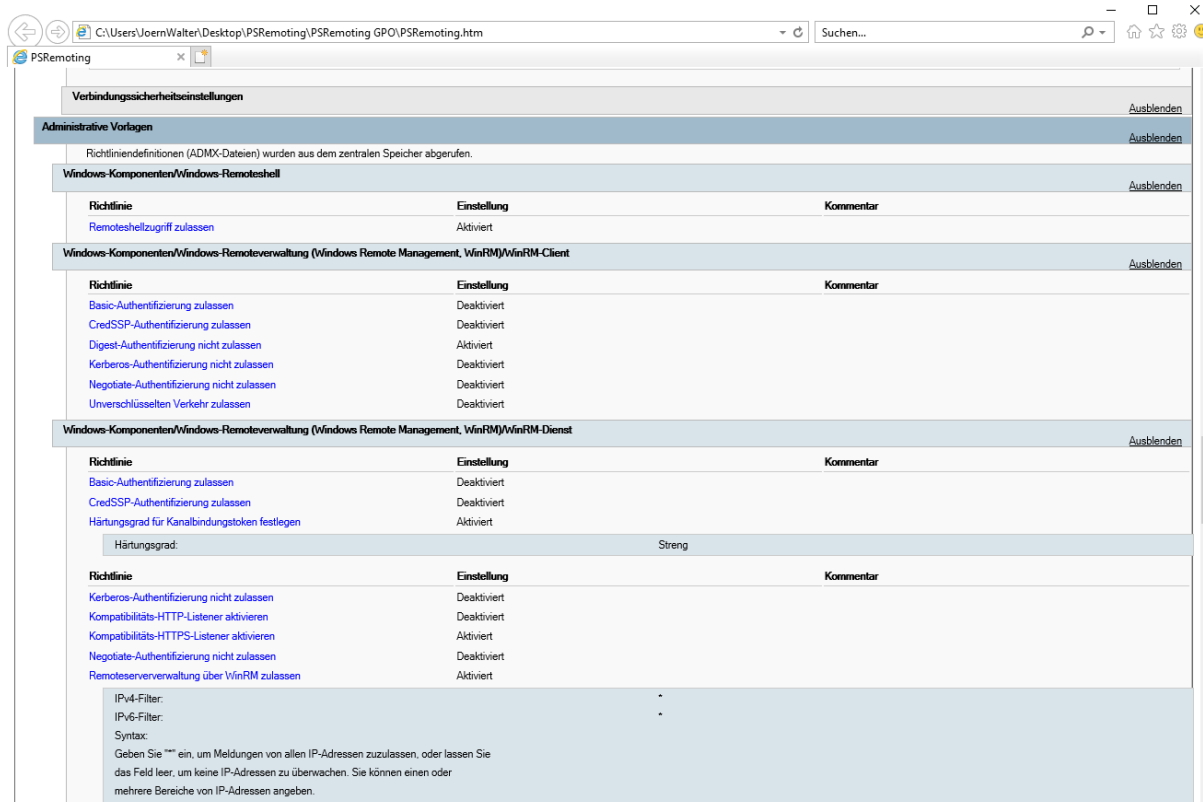


PSRemoting aktivieren

Das Ziel ist es, alle Windows Computer aus der Ferne sicher steuern zu können. Zum Einsatz kommt hier das Protokoll (Web Services for Management) WSMa. Es ist sicher und einfach anzuwenden und wir bauen bei der Authentifizierung auf die Nutzung von TLS-Zertifikaten. Bevor man loslegen kann, muss erst einmal die Remote Verwaltung WINRM (Windows Remote Management) konfiguriert werden.

Über ein Gruppenrichtlinienobjekt nehmen wir die lokale Konfiguration der Systeme vor.

- Authentifizierung
- Firewall
- Services
- Listener



Darüber hinaus verteilen wir über die interne Zertifizierungsstelle Zertifikate an jedes System.

Die Umsetzung erfolgt mittels einer dafür eingerichtete Zertifikatsvorlage und eine separate Richtlinie.



PSRemoting aktivieren

Hier sehen wir die WinRM Standardkonfiguration eines Server Systems.

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>winrm e winrm/config/listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.112, ::1

C:\Windows\system32>_
```

Hier sehen wir, dass Einfluss auf die Konfiguration mittels einer Richtlinie genommen wurde.

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>winrm e winrm/config/listener
Listener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1

Listener [Source="Compatibility"]
  Address = *
  Transport = HTTPS
  Port = 443
  Hostname = DC1.dwp.local
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1

C:\Windows\system32>_
```



PSRemoting aktivieren

Hier sehen wir eine Konfiguration, die ein Zertifikat zur Authentifizierung einsetzt.

```
Administrator: Eingabeaufforderung
C:\Windows\system32>winrm e winrm/config/listener
Listener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1

Listener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = 19842D95898277FBEABD41AB09B1E387801D2361
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1

Listener [Source="Compatibility"]
  Address = *
  Transport = HTTPS
  Port = 443
  Hostname = DC1.dwp.local
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1
```

Kommen wir zur Umsetzung:

Zertifikatsvorlage auf der Zertifizierungsstelle einrichten.

The image shows two screenshots of the 'Eigenschaften von WSMAN' (WSMAN Properties) dialog box. The left screenshot shows the 'Allgemein' (General) tab with the following settings: 'Vorlagenanzeigenname' (Template display name) is 'WSMAN', 'Vorlagenname' (Template name) is 'WSMAN', 'Gültigkeitsdauer' (Validity period) is 1 year, and 'Erneuerungszeitraum' (Renewal period) is 2 days. The right screenshot shows the 'Kryptografie' (Cryptography) tab with the following settings: 'Anbieterkategorie' (Provider category) is 'Schlüsselspeicheranbieter' (Key storage provider), 'Name des Algorithmus' (Algorithm name) is 'RSA', 'Minimale Schlüsselgröße' (Minimum key size) is 2048, 'Auswählen der für Anforderungen verwendbaren Kryptografieanbieter' (Select cryptography providers for requirements) is set to 'Verwendung aller auf dem Computer des Antragstellers verfügbaren Anbieter für Anforderungen möglich' (Use all providers available on the requester's computer for requirements), 'Anbieter' (Providers) list includes 'Microsoft Software Key Storage Provider', 'Microsoft Platform Crypto Provider', and 'Microsoft Smart Card Key Storage Provider', 'Anforderungshash' (Requirement hash) is 'SHA256', and 'Alternatives Signaturformat verwenden' (Use alternative signature format) is unchecked.



PSRemoting aktivieren

The image shows two screenshots of the 'Eigenschaften von WSMAN' (WSMAN Properties) dialog box. The left screenshot shows the 'Erweiterungen' (Extensions) tab, where 'Anwendungsrichtlinien' (Application Policies) is selected. The right screenshot shows the 'Sicherheit' (Security) tab, where 'Aus diesen Informationen in Active Directory erstellen' (Create from information in Active Directory) is selected. Both screenshots show the 'Abbrechen' (Cancel) button highlighted.

Die Vorlage wird veröffentlicht.

The image shows a screenshot of the 'Konsolenstamm' (Console Root) window. The 'Zertifikatsvorlagen' (Certificate Templates) folder is expanded, and the 'WSMAN' template is highlighted with a red arrow. The 'WSMAN' template is listed with the purpose 'Serverauthentifizierung' (Server Authentication).



PSRemoting aktivieren

Für die automatische Verteilung (Registrierung) und Erneuerung von Zertifikaten (WSMAN) benötigen wir eine Richtlinie.

The screenshot shows the 'Group Policy Management' console with the 'Certificates' policy selected. The policy is currently set to 'Not Configured'. The 'Details' tab is active, showing the following settings:

- Sicherheitsfilterung:** The settings for this Group Policy object can only be applied to the following groups, users, and computers:
 - Name: NT-AUTORITÄT\Authentifizierte Benutzer
- Delegation:** The following groups and users have the specified permissions for this Group Policy object:

Name	Zulässige Berechtigungen	Geerbt
DWP\Domain-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
DWP\Organisation-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
- Computerkonfiguration (Aktiviert):**
 - Richtlinien:** Ausblenden
 - Windows-Einstellungen:** Ausblenden
 - Sicherheitseinstellungen:** Ausblenden
 - Richtlinien für öffentliche Schlüssel/Zertifikatsdienst - Einstellung für die automatische Registrierung:** Ausblenden
 - Richtlinie:** Automatische Zertifikatsverwaltung, **Einstellung:** Aktiviert
 - Option:** Neue Zertifikate registrieren; abgelaufene Zertifikate erneuern, ausstehende Anforderungen für Zertifikate verarbeiten und gesperrte Zertifikate entfernen, **Einstellung:** Aktiviert
 - Zertifikate, die Zertifikatsvorlagen von Active Directory verwenden, aktualisieren und verwalten:** Aktiviert
- Benutzerkonfiguration (Aktiviert):** Ausblenden
 - Keine Einstellungen definiert

The screenshot shows the 'Group Policy Management' console with the 'Certificates' policy selected. The 'Verknüpfungen' tab is active, showing the following settings:

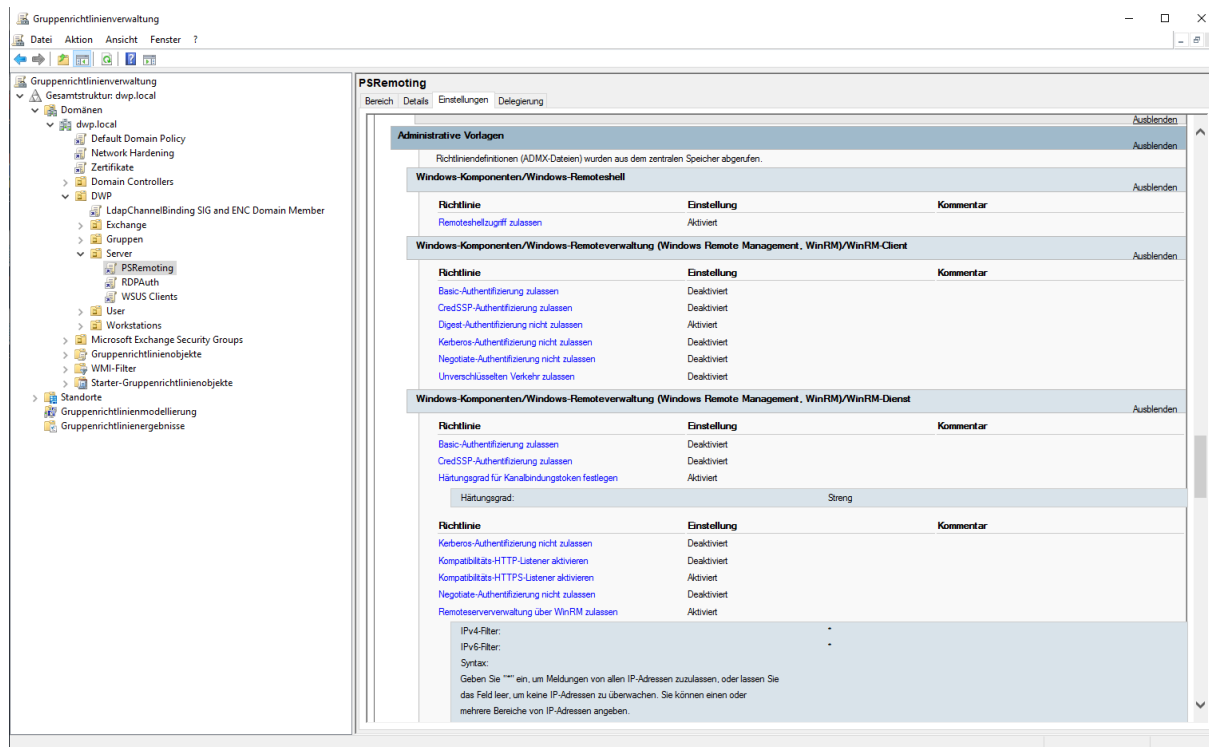
- Verknüpfungen:** Für dieses Verzeichnis anzeigen: dwp.local. Die folgenden Standorte, Domänen und Organisationseinheiten sind mit dem Objekt verknüpft:

Standort	Erzwingen	Verknüpfung aktiviert	Pfad
dwp.local	Nein	Ja	dwp.local
- Sicherheitsfilterung:** Die Einstellungen dieses Gruppenrichtlinienobjekts gelten nur für die folgenden Gruppen, Benutzer und Computer:
 - Name: Authentifizierte Benutzer
- WMI-Filterung:** Dieses Gruppenrichtlinienobjekt ist mit folgendem WMI-Filter verknüpft:
 - <Kein>



PSRemoting aktivieren

Zum Abschluss erstellen wir die Gruppenrichtlinie zur Konfiguration von WSMAN, der Firewall, der Authentifizierung und der Listener als geplante Aufgabe.

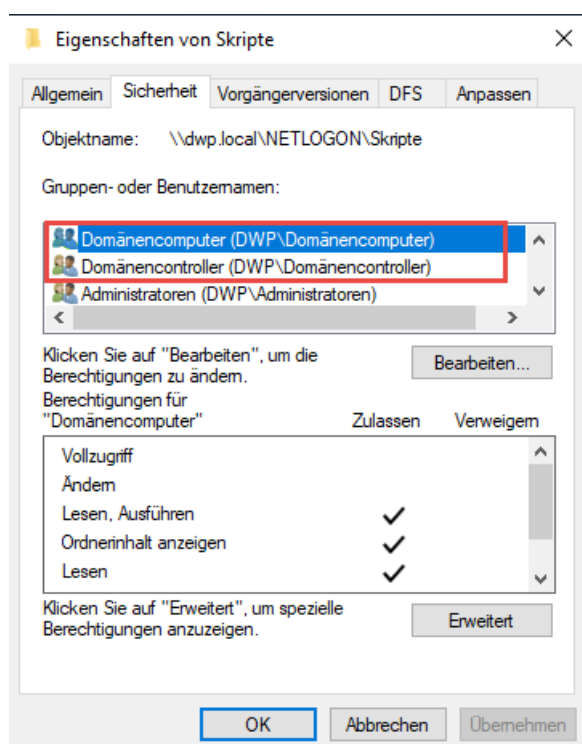
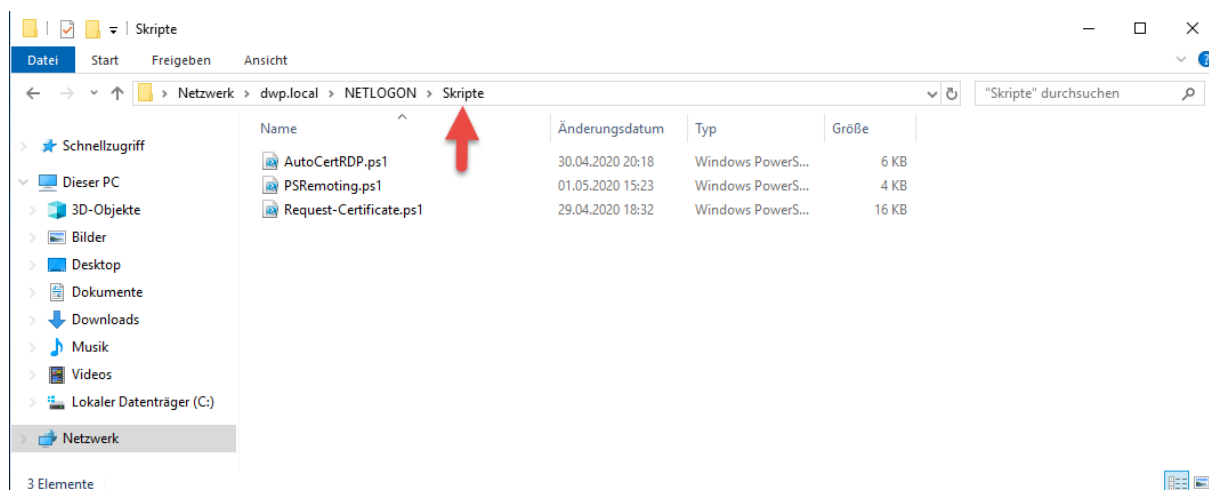


Das Skript befindet sich in meinem Lab im Ordner Skripte unter Netlogon.

```
56 }
57
58 $Event = Test-EventLog "PSRemoting"
59
60 If ($Event -eq $false) {
61
62   New-EventLog -LogName Application -Source "PSRemoting"
63
64   Write-EventLog -LogName Application -Source "PSRemoting" -EntryType Information -EventId 0 -Message "Die Event-Source PSRemoting wurde angelegt."
65 }
66
67 # Zertifikatspeicher festlegen
68 $certLocation = "LocalMachine\My"
69 # Funktion zum Auslesen der Erweiterung
70 function get-InstalledCertificateInfo($certLocation) {
71
72   $array = gci Cert:\$certLocation | `
73     select Thumbprint, `
74     @{
75       $p="CN";e=((($_.Subject).split(",")[1]), `
76       # Bei einem englischen OS -match Template
77       $p="IssuedFromTemplate";e=[regex]:match(($_.extensions.Format(0)) | ? { $_ -match "Vorlage" }).split(",")[0] , '^(Vorlage=)(\w.*)(\{[0-9]*\})$'.Groups[2].value}}
78     return $array
79 }
80
81 # Variablen setzen
82 $WinRMcertFound = $false
83 $WinRMcertTemplateName = "WSMAN"
84
85 $timeout = New-TimeSpan -Seconds 90
86 $endTime = (Get-Date).Add($timeout)
87 # Aufgabe zur Ermittlung des Fingerprints der oben genannten Zertifikatsvorlage
88 # Ist ein Zertifikat basierend auf der Vorlage vorhanden wird es an den HTTPS Listener gebunden
89 do {
90
91   if (Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }) {
92     $WinRMcertThumbprint = ((Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }).Thumbprint).replace(" ", "").toupper()
93     $WinRMcertCN = (Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }).CN
94     Write-EventLog -LogName Application -Source "PSRemoting" -EntryType Information -EventId 1 -Message "Ein Zertifikat basierend auf das Template $WinRMcertTemplateName mit dem Thumbprint $WinRMcertThumbprint wurde im Computerspeicher gefunden" -ForegroundColor Cyan
95     $WinRMcertFound = $true
96
97     Write-Host "Der HTTPS Listener wird neu konfiguriert" -ForegroundColor Cyan
98     WinRM delete winrm/config/Listener?Address=*+Transport=HTTPS
99     New-Item WinRM:\localhost\Listener -Transport HTTPS -Address * -CertificateThumbprint $WinRMcertThumbprint -Force
100     Write-EventLog -LogName Application -Source "PSRemoting" -EntryType Information -EventId 2 -Message "Der Thumbprint $WinRMcertThumbprint wurde an den HTTPS Listener gebunden"
101   }
```



PSRemoting aktivieren



Das Skript sorgt dafür, dass das Zertifikat aus der Vorlage WSMAN immer an den HTTPS Listener gebunden wird/bleibt, auch nach einer Erneuerung des Zertifikats.

Wie lange bei euch ein Zertifikat gültig ist und wie oft ihr den Task laufen lasst, sollte jeder für sich entscheiden.

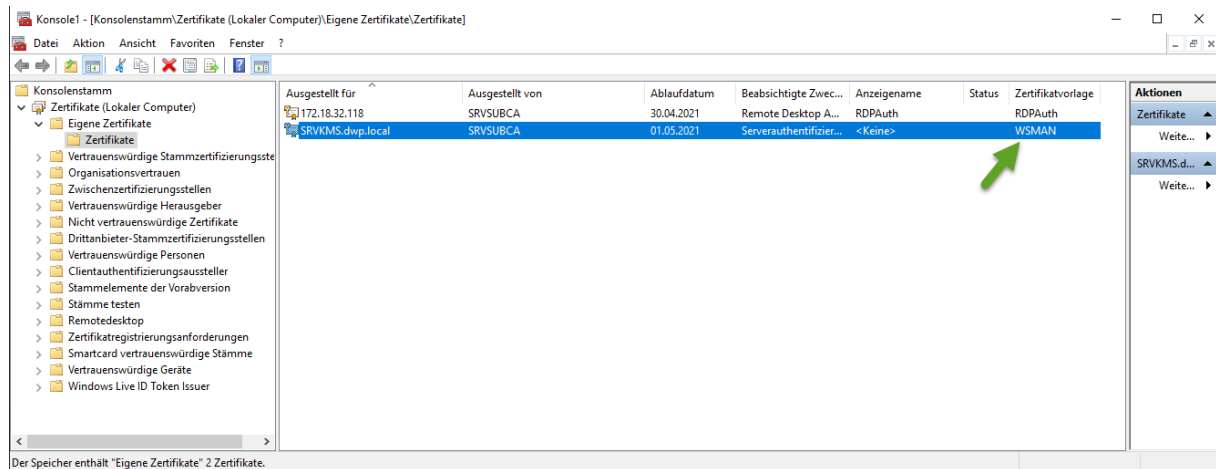
Mit dieser Methode habe ich für mich eine brauchbare Lösung gefunden.



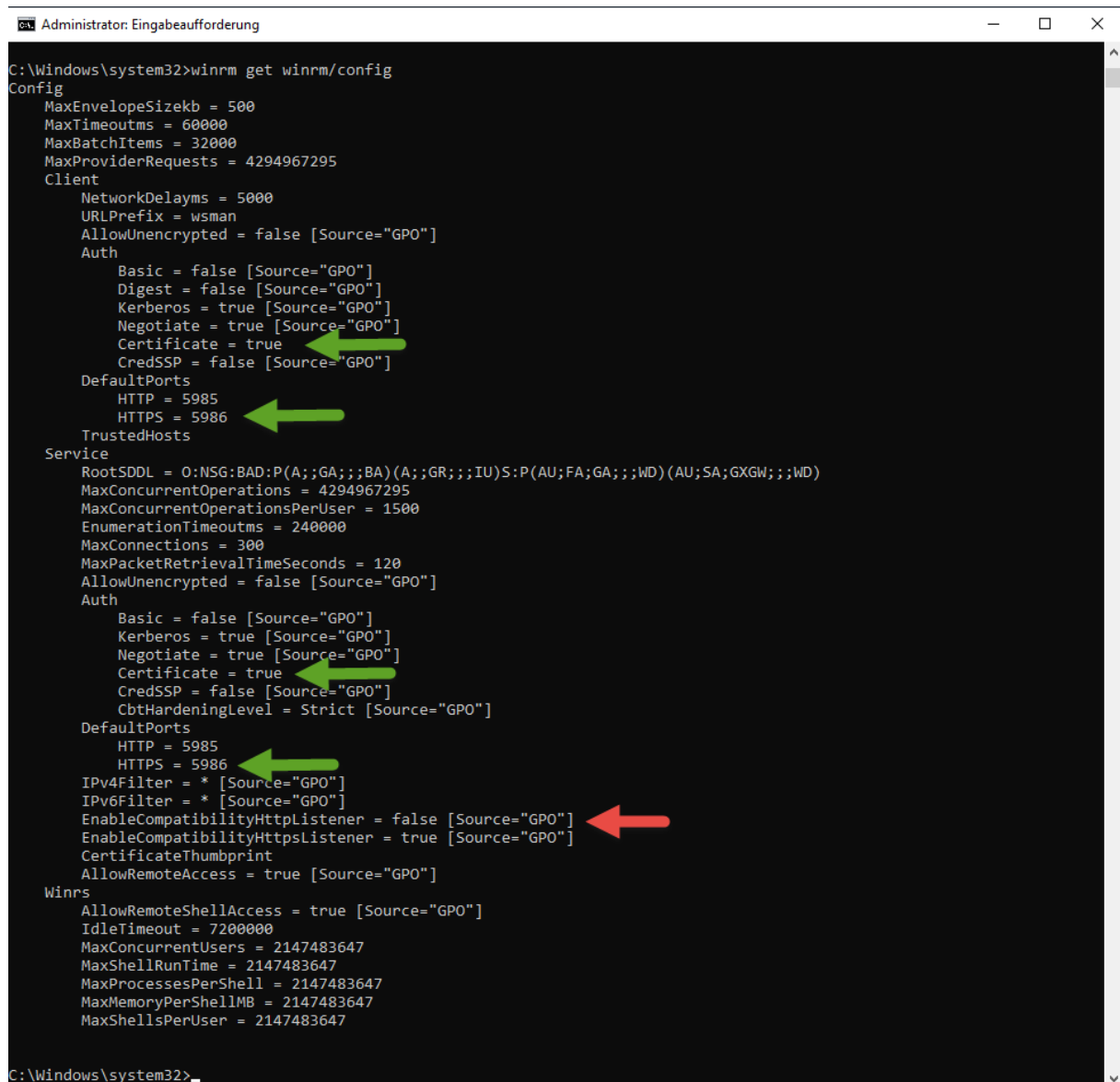
PSRemoting aktivieren

Nachdem alles umgesetzt wurde, sieht das Ergebnis wie folgt aus:

Es existiert ein Zertifikat auf Basis der Vorlage namens WSMAN.



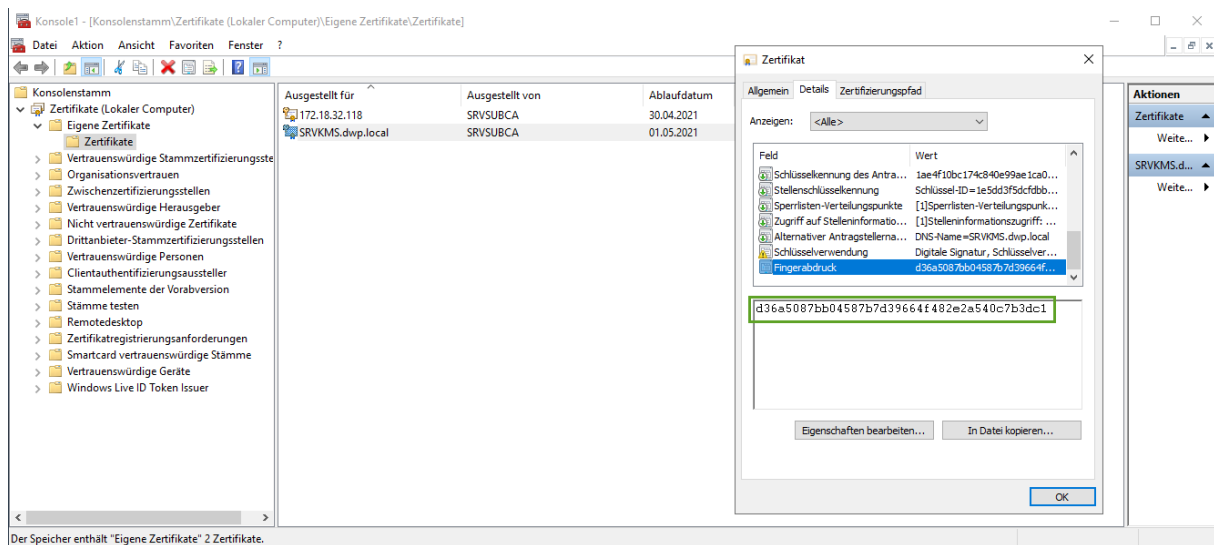
winrm get winrm/config



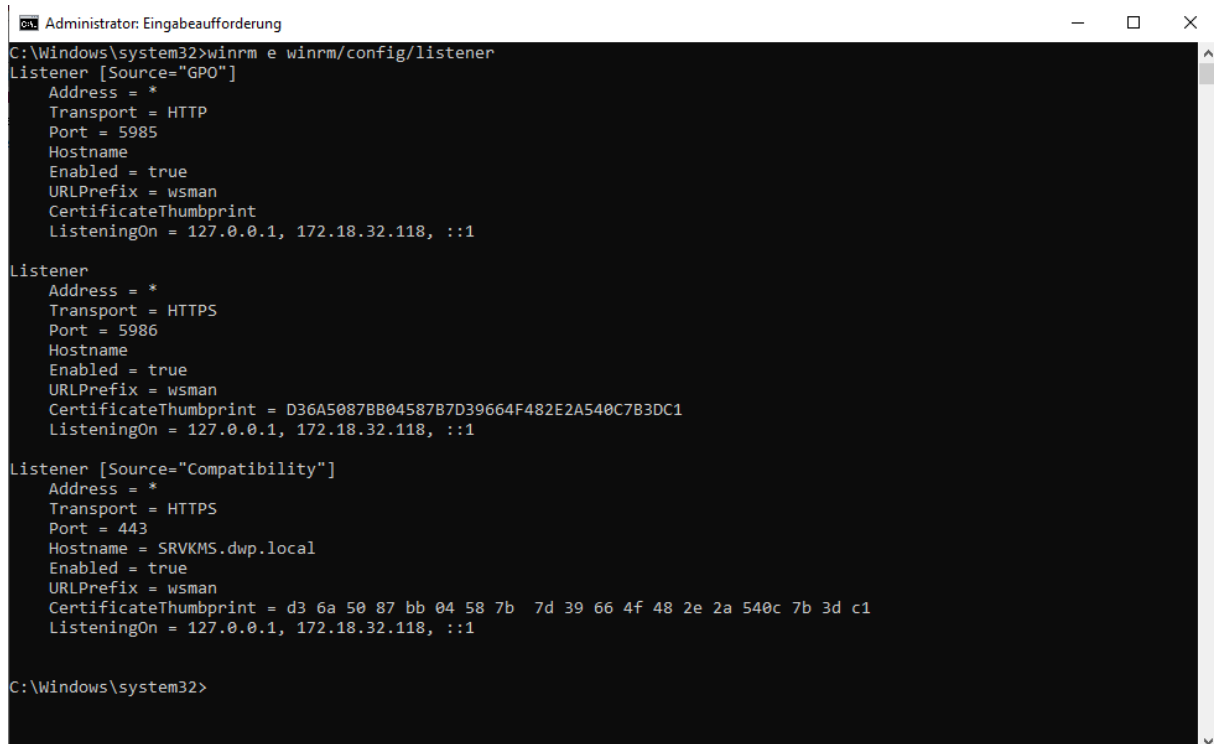


PSRemoting aktivieren

Das individuelle „WSMAN“ Zertifikat,



wurde ordnungsgemäß an WSMAN gebunden.





PSRemoting aktivieren

Der Test bestätigt die saubere Umsetzung.

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Test WSMAN.ps1* X
1 Enter-PSSession -ComputerName SRVSubCA.dwp.local
2 Enter-PSSession -ComputerName SRVSubCA.dwp.local -UseSSL

PS C:\Windows\system32> Enter-PSSession -ComputerName SRVSubCA.dwp.local
Enter-PSSession : Beim Verbinden mit dem Remoteserver "SRVSubCA.dwp.local" ist folgender Fehler aufgetreten: WinRM kann den Vorgang nicht abschließen. Überprüfen Sie, ob der angegebene Computername gültig, der Computer über das Netzwerk erreichbar und eine Firewallausnahme für den WinRM-Dienst aktiviert ist und den Zugriff von diesem Computer zulässt. Standardmäßig wird der Zugriff auf Remotecomputer innerhalb desselben lokalen Subnetzes von der WinRM-Firewallausnahme für öffentliche Profile eingeschränkt. Weitere Informationen finden Sie im Hilfethema "about_Remote_Troubleshooting".
In Zeile:1 Zeichen:1
+ Enter-PSSession -ComputerName SRVSubCA.dwp.local
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (SRVSubCA.dwp.local:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed

PS C:\Windows\system32> Enter-PSSession -ComputerName SRVSubCA.dwp.local -UseSSL
[SRVSubCA.dwp.local]: PS C:\Users\JW\Documents>
```

Zum Testen:

Enter-PSSession -CN SRVSubCA.dwp.local # Fehler wegen fehlender SSL Nutzung
Enter-PSSession -CN SRVSubCA.dwp.local -UseSSL

Stop-Service spooler

Get-Service spooler

Start-Service spooler

Restart-Service spooler

Exit-PSSession

Enter-PSSession -CN SRVSubCA.dwp.local -UseSSL -Authentication Kerberos

Exit-PSSession

New-PSSession -CN SRVSubCA.dwp.local -UseSSL -Authentication Kerberos

Enter-PsSession -ID 9

Exit-PSSession

Remove-PSSession -ID 9

Get-PSSession | Disconnect-PSSession

Invoke-Command -CN SRVKMS.dwp.local,SRVSubCA.dwp.local -UseSSL -ScriptBlock {Get-Service spooler}

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

PSBefehle.ps1 X
18 Invoke-Command -CN SRVKMS.dwp.local,SRVSubCA.dwp.local -UseSSL -ScriptBlock {Get-Service spooler}

PS C:\Windows\system32> Invoke-Command -CN SRVKMS.dwp.local,SRVSubCA.dwp.local -UseSSL -ScriptBlock {Get-Service spooler}

Status Name DisplayName PSComputerName
-----
Running spooler Druckwarteschlange SRVSubCA.dwp.local
Running spooler Druckwarteschlange SRVKMS.dwp.local

PS C:\Windows\system32>
```