



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

The screenshot shows the Group Policy Editor window titled "PSRemoting". The left pane shows the hierarchy: "Verbindungssicherheitseinstellungen" > "Administrative Vorlagen" > "Windows-Komponenten/Windows-Remoteshell" > "Windows-Komponenten/Windows-Remoteverwaltung (Windows Remote Management, WinRM)/WinRM-Client" > "Windows-Komponenten/Windows-Remoteverwaltung (Windows Remote Management, WinRM)/WinRM-Dienst".

Richtlinie	Einstellung	Kommentar
Remoteshellzugriff zulassen	Aktiviert	
Basic-Authentifizierung zulassen	Deaktiviert	
CredSSP-Authentifizierung zulassen	Deaktiviert	
Digest-Authentifizierung nicht zulassen	Aktiviert	
Kerberos-Authentifizierung nicht zulassen	Deaktiviert	
Negotiate-Authentifizierung nicht zulassen	Deaktiviert	
Unverschlüsselten Verkehr zulassen	Deaktiviert	

Richtlinie	Einstellung	Kommentar
Basic-Authentifizierung zulassen	Deaktiviert	
CredSSP-Authentifizierung zulassen	Deaktiviert	
Härtungsgrad für Kanalbindungsloken festlegen	Aktiviert	
Härtungsgrad:	Streng	
Kerberos-Authentifizierung nicht zulassen	Deaktiviert	
Kompatibilitäts-HTTP-Listener aktivieren	Deaktiviert	
Kompatibilitäts-HTTPS-Listener aktivieren	Aktiviert	
Negotiate-Authentifizierung nicht zulassen	Deaktiviert	
Remoteserververwaltung über WinRM zulassen	Aktiviert	

IPv4-Filter: -
IPv6-Filter: -
Syntax:
Geben Sie "" ein, um Meldungen von allen IP-Adressen zuzulassen, oder lassen Sie das Feld leer, um keine IP-Adressen zu überwachen. Sie können einen oder mehrere Bereiche von IP-Adressen angeben.

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.

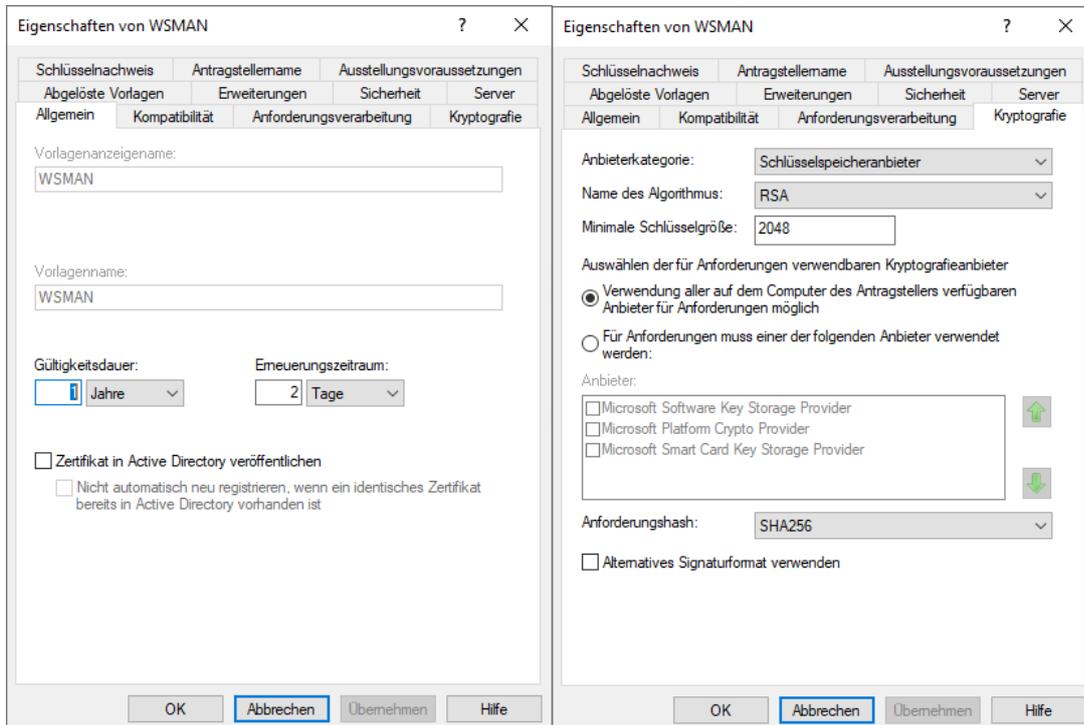
```
Administrator: Eingabeaufforderung
C:\Windows\system32>winrm e winrm/config/listener
Listener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.31, ::1

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
```

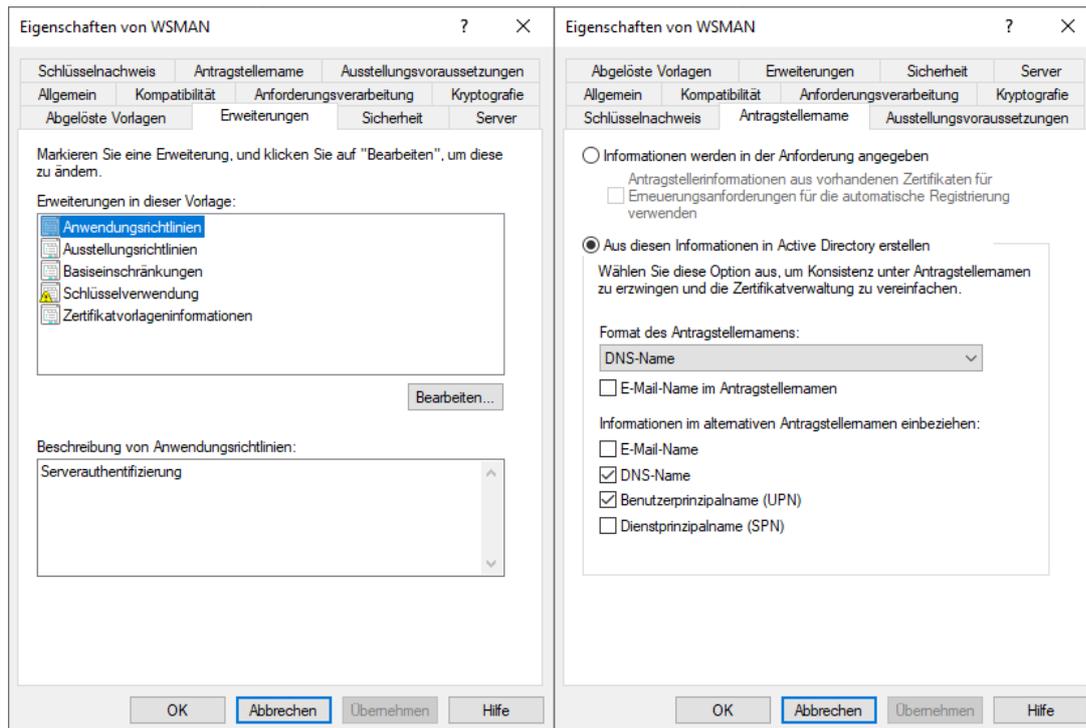
Kommen wir zur Umsetzung:

Zertifikatsvorlage auf der Zertifizierungsstelle einrichten.

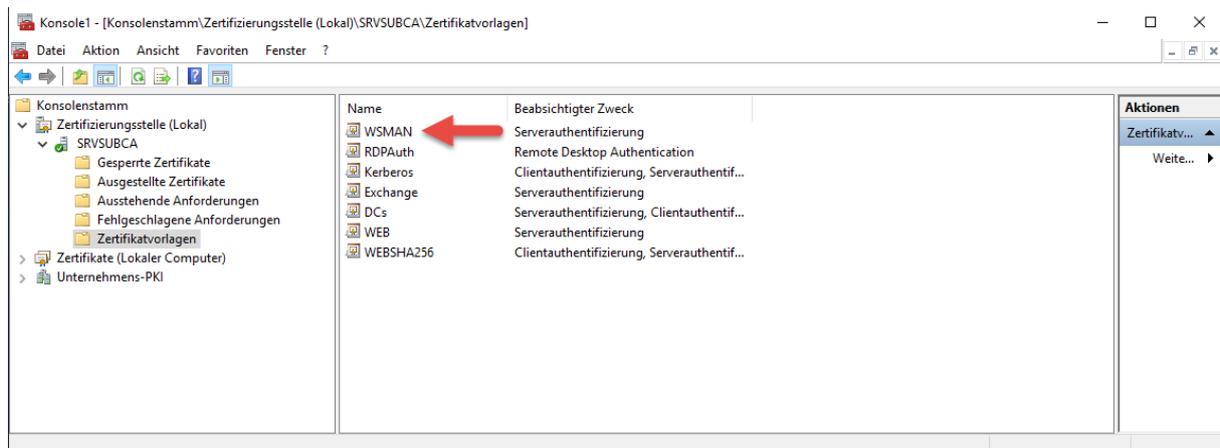




PSRemoting aktivieren



Die Vorlage wird veröffentlicht.





PSRemoting aktivieren

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

The screenshot shows the Group Policy Management console for the domain dwp.local. The left pane shows the tree structure with 'Zertifikate' selected under 'DWP'. The right pane shows the 'Zertifikate' policy configuration.

Zertifikate
Bereich: Details | Einstellungen | Delegation | Status

Objekt	Erzwingen	Verknüpfung aktiviert	Pfad
dwp	Nein	Aktiviert	dwp.local
DWP	Nein	Aktiviert	dwp.local/DWP

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung
Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name	Größe
NT-AUTORITAT\authentifizierte Benutzer	Nein

Delegation
Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerb
DWP\Domain-Admins	Erstellungen bearbeiten, löschen, Sicherheit ändern	Nein
DWP\Organisations-Admins	Erstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITAT\authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITAT\DOMANENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITAT\SYSTEM	Erstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerskonfiguration (Aktiviert)

Richtlinien

Windows-Einstellungen

Sicherheitsfilterung

Richtlinien für öffentliche Schlüssel/Zertifikatsdienstclient - Einstellung für die automatische Registrierung

Richtlinie	Einstellung
Automatische Zertifikatsverwaltung	Aktiviert
Option	Erstellung
Neue Zertifikate registrieren; abgelaufene Zertifikate erneuern, ausstehende Anforderungen für Zertifikate verarbeiten und gesperrte Zertifikate entfernen	
Zertifikate, die Zertifikatsvorlagen von Active Directory verwenden, aktualisieren und verwalten	Aktiviert

Benutzerkonfiguration (Aktiviert)

Keine Einstellungen definiert

The screenshot shows the Group Policy Management console for the domain dwp.local. The left pane shows the tree structure with 'Zertifikate' selected under 'DWP'. The right pane shows the 'Zertifikate' policy configuration with the 'Verknüpfungen' tab selected.

Zertifikate
Bereich: Details | Einstellungen | Delegation

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

Hinzufügen... Entfernen Eigenschaften

WMI-Filterung
Dieses Gruppenrichtlinienobjekt ist mit folgendem WMI-Filter verknüpft:

WMI-Filter
<Kein>

Öffnen



PSRemoting aktivieren

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

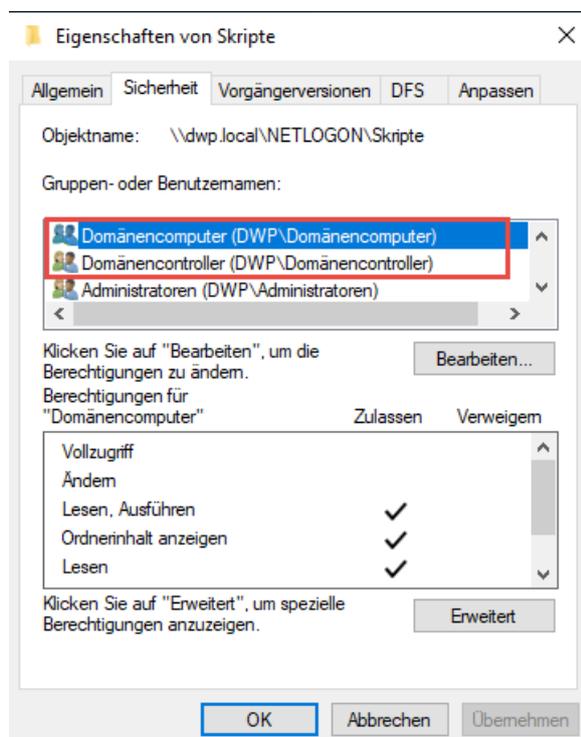
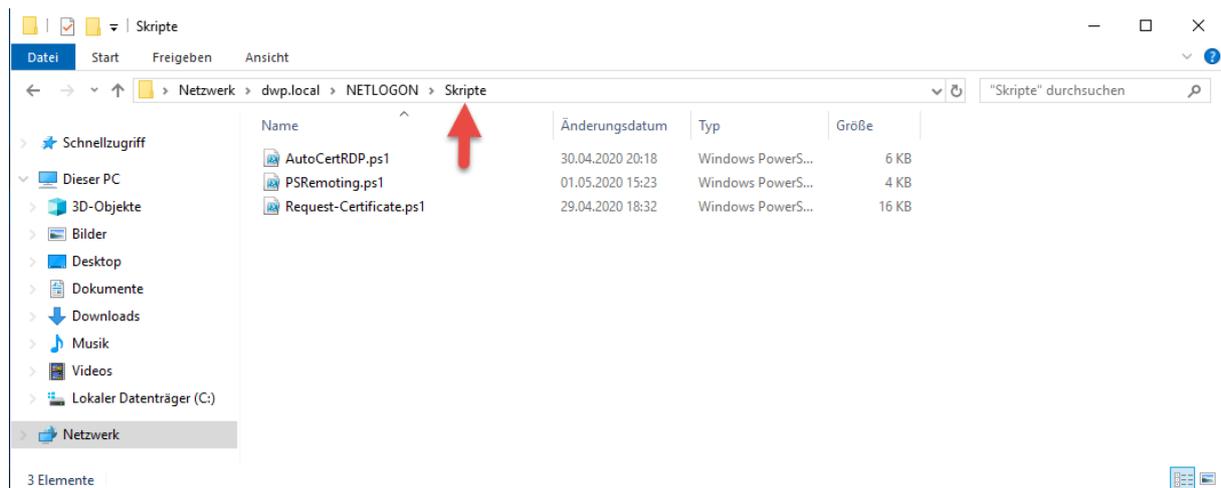
The screenshot shows the Group Policy Management console. The left pane displays the tree structure with 'PSRemoting' selected under 'DWP'. The right pane shows the 'PSRemoting' settings, including 'Administrative Vorlagen', 'Windows-Komponenten/Windows-Remoteshell', 'Windows-Komponenten/Windows-Remoteverwaltung (Windows Remote Management, WinRM)/WinRM-Client', and 'Windows-Komponenten/Windows-Remoteverwaltung (Windows Remote Management, WinRM)/WinRM-Dienst'. The 'Härtungsgrad' is set to 'Streng'.

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     $array = gci Cert:\$certLocation | `
72     select Thumbprint, `
73     @{
74         $[n="CN"]={($_.Subject).split(",")[1]}
75     }
76     # Bei einem englischen OS -match Template
77     @{[n="IssuedFromTemplate"]={($_.extensions.Format(0) | ? { $_ -match "Vorlage" }).split(",")[0] , ''(Vorlage=(\w.*\{[0-9-]*\})$')} }
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     if (Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }) {
91         $WinRMCorporateCertThumbprint = (Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }).Thumbprint).replace(" ", "").toupper()
92         $WinRMCorporateCertCN = (Get-InstalledCertificateInfo $certLocation | ? { $_.IssuedFromTemplate -eq $WinRMcertTemplateName }).CN
93         Write-EventLog -LogName Application -Source "PSRemoting" -EntryType Information -EventId 1 -Message "Ein Zertifikat basierend auf dem Template $WinRMcertTemplateName mit dem Thumbprint $WinRMCorporateCertThumbprint wurde im Computerspeicher gefunden" -ForegroundColor Cyan
94         $WinRMcertFound = $true
95     }
96
97     Write-Host "Der HTTPS Listener wird neu konfiguriert" -ForegroundColor Cyan
98     winrm get winrm/config/Listener?Address=*+Transport=HTTPS
99     New-Item WSMAN:\localhost\Listener -Transport HTTPS -Address * -CertificateThumbprint $WinRMCorporateCertThumbprint -Force
100     Write-EventLog -LogName Application -Source "PSRemoting" -EntryType Information -EventId 2 -Message "Der Thumbprint $WinRMCorporateCertThumbprint 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.

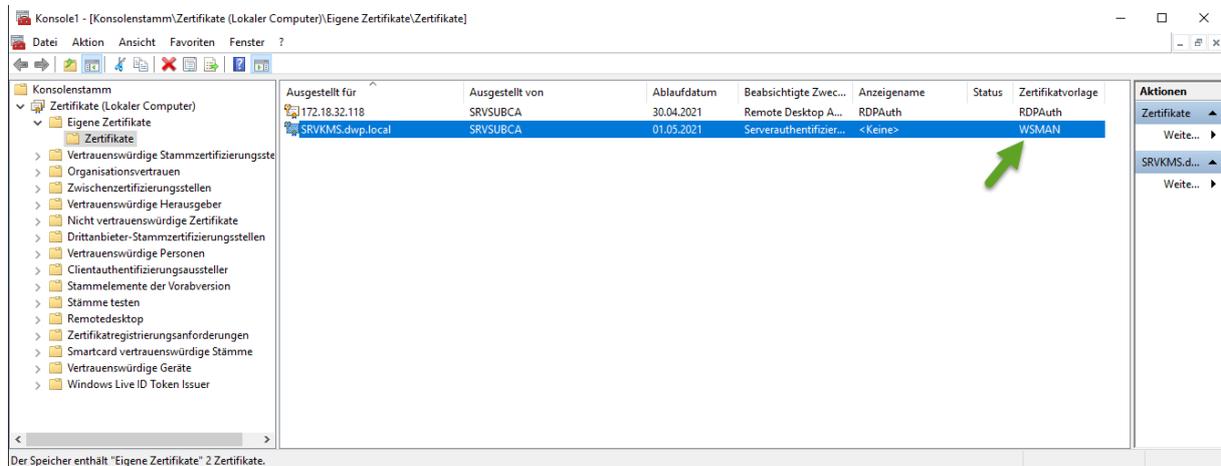
Mit dieser Methode habe ich für mich eine brauchbare Lösung gefunden.



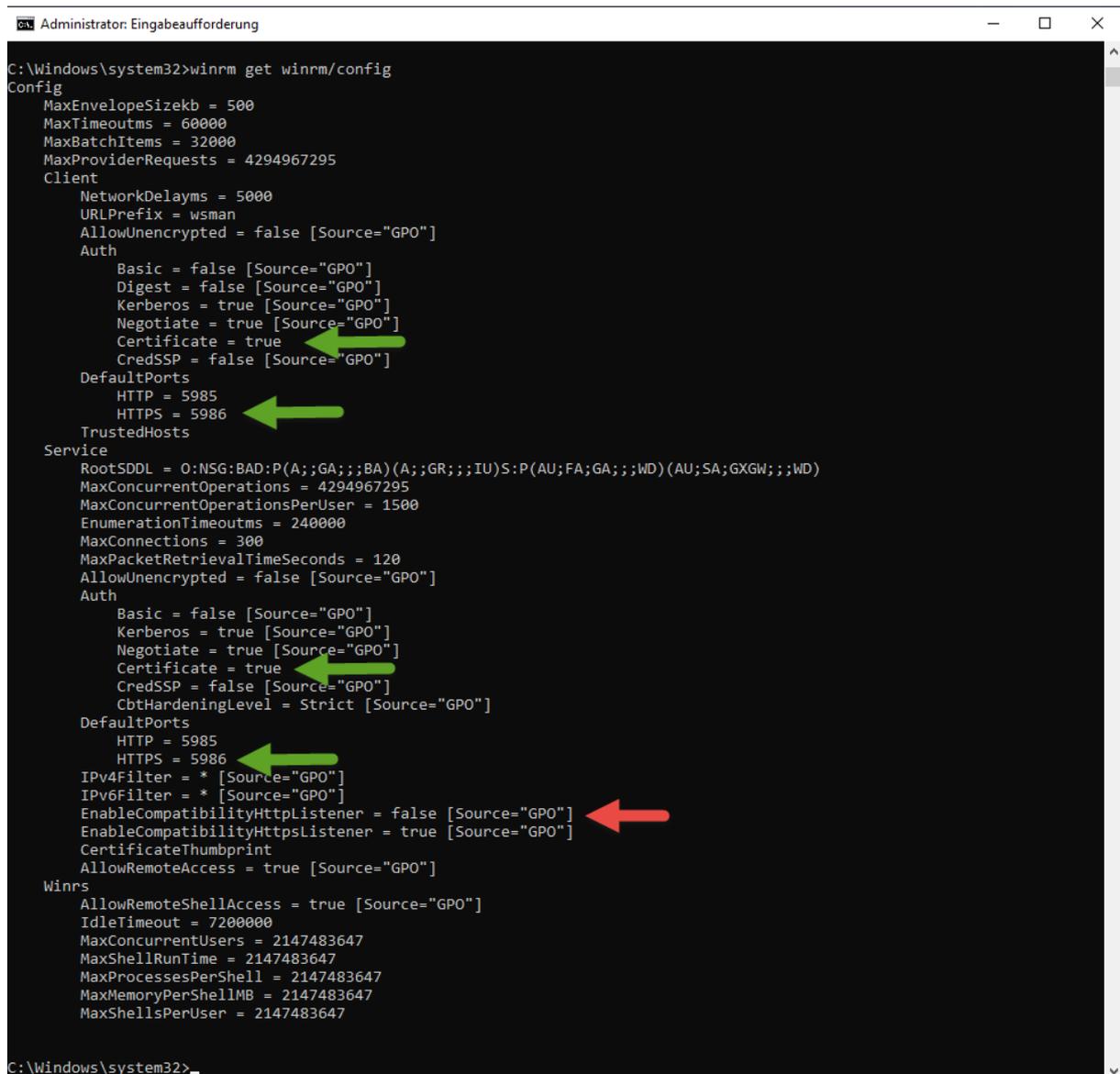
PSRemoting aktivieren

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

Es existiert ein Zertifikat auf Basis der Vorlage namens WSMAN.



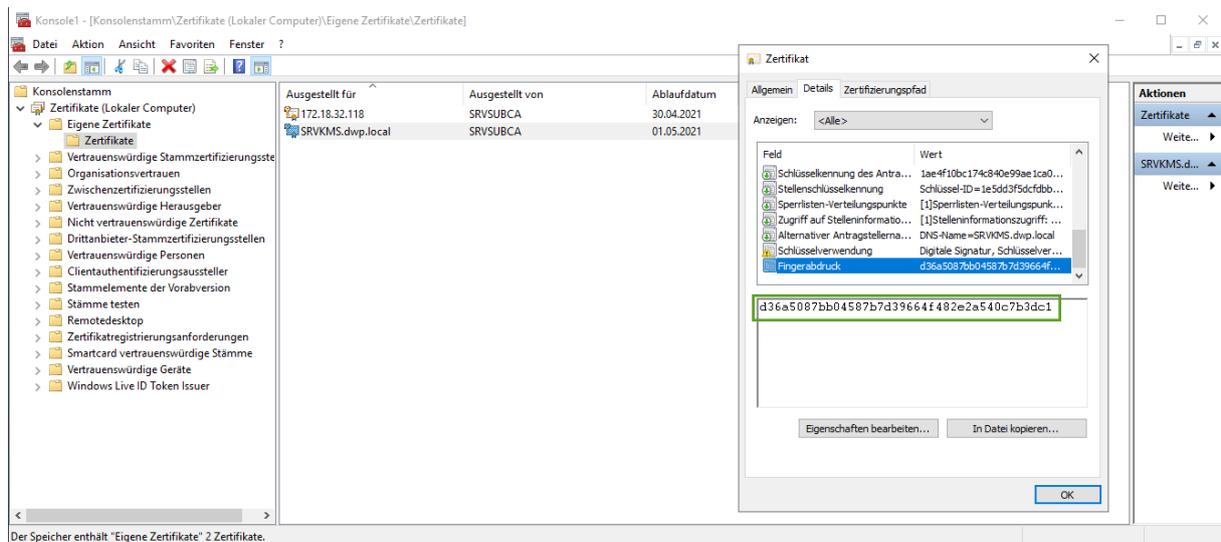
winrm get winrm/config





PSRemoting aktivieren

Das individuelle „WSMAN“ Zertifikat,



wurde ordnungsgemäß an WSMAN gebunden.

```
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, 172.18.32.118, ::1

Listener
  Address = *
  Transport = HTTPS
  Port = 5986
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = D36A5087BB04587B7D39664F482E2A540C7B3DC1
  ListeningOn = 127.0.0.1, 172.18.32.118, ::1

Listener [Source="Compatibility"]
  Address = *
  Transport = HTTPS
  Port = 443
  Hostname = SRVKMS.dwp.local
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = d3 6a 50 87 bb 04 58 7b 7d 39 66 4f 48 2e 2a 540c 7b 3d c1
  ListeningOn = 127.0.0.1, 172.18.32.118, ::1

C:\Windows\system32>
```



PSRemoting aktivieren

Der Test bestätigt die saubere Umsetzung.

The screenshot shows the Windows PowerShell ISE interface. The command prompt shows two commands: `Enter-PSSession -ComputerName SRVSubCA.dwp.local` and `Enter-PSSession -ComputerName SRVSubCA.dwp.local -UseSSL`. The first command fails with an error message: "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". The second command succeeds, showing the prompt `[SRVSubCA.dwp.local]: PS C:\Users\JW\Documents>`. Red and green callouts highlight the difference: "geht nicht ohne SSL" points to the first command, and "geht per SSL" points to the second command.

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}`

The screenshot shows the Windows PowerShell ISE interface. The command prompt shows the command: `Invoke-Command -CN SRVKMS.dwp.local,SRVSubCA.dwp.local -UseSSL -ScriptBlock {Get-Service spooler}`. The output shows a table with columns: Status, Name, DisplayName, and PSComputerName. The table contains two rows: one for 'spooler' on 'SRVSubCA.dwp.local' and one for 'spooler' on 'SRVKMS.dwp.local', both with a status of 'Running'.

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