PowerShell Remoting i WinRM – Porty i Szyfrowanie

Windows Remote Management (WinRM) to mechanizm komunikacji sieciowej oparty na protokole WS-Management, który umożliwia zdalne zarządzanie maszynami Windows. PowerShell Remoting wykorzystuje WinRM do wykonywania poleceń i skryptów na zdalnych hostach.

Domyślne porty WinRM

- Port 5985: HTTP (połączenia nieszyfrowane)
- Port 5986: HTTPS (połączenia szyfrowane – wymagany certyfikat SSL)
- Porty 80 i 443 mogą być używane w starszych konfiguracjach, ale obecnie standardem są 5985 i 5986.

Standardowe działanie

Po uruchomieniu PowerShell Remoting przy pomocy polecenia:

```
Enable-PSRemoting -Force
```

WinRM konfiguruje słuchacza na porcie 5985 (HTTP). Połączenia są nieszyfrowane, ale mogą być bezpieczne w środowiskach domenowych, gdzie zabezpieczenia Kerberos zapewniają uwierzytelnienie i poufność danych.

Wymuszenie szyfrowania (HTTPS)

Aby wymusić szyfrowane połączenia PowerShell Remoting:

1. Zainstaluj certyfikat SSL na komputerze docelowym.
2. Skonfiguruj słuchacza HTTPS:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname='host.fqdn'; CertificateThumbprint='thumbprint'}
```

lub użyj skrótu:

```
winrm quickconfig -transport:https
```

3. Otwórz port 5986 w zaporze sieciowej:

```
netsh advfirewall firewall add rule name="WinRM HTTPS" dir=in action=allow
protocol=TCP localport=5986
```

4. Upewnij się, że klient używa odpowiedniego protokołu:

```
Enter-PSSession -ComputerName host.fqdn -UseSSL
```

Sprawdzenie konfiguracji

Aby sprawdzić aktywnych słuchaczy WinRM:

```
winrm enumerate winrm/config/listener
```

Aby sprawdzić stan usługi WinRM:

```
Get-Service WinRM
```