Włączanie PowerShell Remoting na stacjach roboczych przez GPO

Poniższy dokument opisuje, jak w środowisku domenowym włączyć PowerShell Remoting na komputerach klienckich (Windows 10 / Windows 11) z wykorzystaniem Grupowej Polityki Zasad (Group Policy Object – GPO). Opis dotyczy konfiguracji wyłącznie z poziomu konsoli GPMC (GUI), bez użycia PowerShell.

1. Założenia i wymagania

- Wszystkie komputery klienckie są członkami domeny Active Directory.

- Na kontrolerze domeny dostępna jest konsola „Group Policy Management" (GPMC).

- Administrator posiada uprawnienia do tworzenia i linkowania obiektów GPO.

- Włączony jest standardowy mechanizm replikacji AD oraz SYSVOL – po zmianach GPO konfiguracja rozpropaguje się na wszystkie kontrolery domeny.

2. Czym jest PowerShell Remoting (WinRM)?

PowerShell Remoting wykorzystuje usługę Windows Remote Management (WinRM), która komunikuję się domyślnie po HTTP na porcie 5985. Włączenie remoting'u na stacjach roboczych pozwala administratorowi uruchamiać komendy i skrypty PowerShell zdalnie, bez konieczności logowania się interaktywnie na każdym komputerze.

Do działania remoting'u konieczne są trzy elementy:
• Usługa WinRM włączona i skonfigurowana (listener).
• Odpowiednia polityka bezpieczeństwa (zezwolenie na zarządzanie przez WinRM).
• Reguła zapory sieciowej zezwalająca na ruch przychodzący na port 5985 (HTTP).

3. Tworzenie nowego obiektu GPO

1. Na kontrolerze domeny uruchom konsolę **Group Policy Management (GPMC).**

2. Rozwiń drzewo domeny, np. „keja.msft".

3. Kliknij prawym przyciskiem myszy na folderze „Group Policy Objects" i wybierz „New…".

4. Wprowadź nazwę nowej polityki, np. „Enable-PSRemoting-Clients" i zatwierdź przyciskiem „OK".

4. Konfiguracja WinRM – Allow remote server management through WinRM

Kolejny krok to skonfigurowanie ustawień usługi WinRM w nowo utworzonym obiekcie GPO.

1. W konsoli GPMC kliknij dwukrotnie nowo utworzony GPO „Enable-PSRemoting-Clients".

2. W drzewie nawigacji wybierz:

Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Remote Management (WinRM) → WinRM Service

3. Odszukaj ustawienie „Allow remote server management through WinRM” i kliknij je dwukrotnie.

4. Ustaw opcję na „Enabled”.

5. W polach filtrów adresów IP skonfiguruj:
- IPv4 filter: *
- IPv6 filter: *

Gwiazdka (*) oznacza, że usługa WinRM będzie nasłuchiwać na wszystkich adresach IP komputera.

6. Zatwierdź ustawienie przyciskiem „OK”.

5. Konfiguracja zapory Windows (Windows Defender Firewall)

Samo włączenie WinRM nie wystarczy, jeśli ruch na porcie 5985 jest blokowany przez zaporę Windows. W tym kroku włączamy predefiniowaną regułę zapory umożliwiającą zdalne zarządzanie.

1. W edycji tego samego GPO przejdź do:
Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall with Advanced Security → Windows Defender Firewall with Advanced Security.

2. Kliknij „Inbound Rules”, następnie w panelu po prawej wybierz „New Rule…”.

3. W kreatorze wybierz opcję „Predefined” i z listy rozwijanej wybierz „Windows Remote Management (HTTP-In)”.

4. Kliknij „Next”, zaznacz „Allow the connection” i zakończ kreator.

W efekcie na komputerach objętych GPO zostanie włączona reguła zapory zezwalająca na połączenia przychodzące do usługi WinRM po HTTP (port 5985).

6. Podlinkowanie GPO do odpowiedniego OU

Aby polityka była stosowana do wskazanych komputerów klienckich, trzeba podlinkować GPO do odpowiedniej jednostki organizacyjnej (OU) w domenie.

1. W konsoli GPMC odnajdź OU, która zawiera komputery klienckie (np. „OU=Komputery”).

2. Kliknij prawym przyciskiem myszy na OU i wybierz „Link an Existing GPO…”.

3. Z listy wybierz GPO „Enable-PSRemoting-Clients” i zatwierdź „OK”.

Od tej chwili wszystkie komputery zlokalizowane w danym OU (oraz w jego pod-OU, o ile dziedziczenie nie jest zablokowane) będą otrzymywać ustawienia WinRM oraz zapory z tej polityki.

7. Replikacja i wymuszenie odświeżenia polityk na kliencie

Po zapisaniu zmian w GPO należy poczekać na replikację Active Directory i SYSVOL. Na stacjach roboczych można przyspieszyć zastosowanie ustawień, uruchamiając polecenie:

```
gpupdate /force
```

Dodatkowo, w środowisku z wieloma kontrolerami domeny administrator może zweryfikować, czy GPO zostało zreplikowane poprawnie, korzystając z narzędzi takich jak „Active Directory Sites and Services" czy „repadmin".

8. Weryfikacja działania PowerShell Remoting

Na jednym z komputerów administracyjnych (np. serwerze lub stacji admina) można zweryfikować, czy remoting działa poprawnie, wykonując zdalne testy po stronie klienta.

1. Sprawdź z poziomu klienta status WinRM, uruchamiając w konsoli (cmd lub PowerShell):
   winrm quickconfig
   Powinien pojawić się komunikat, że usługa WinRM jest skonfigurowana i gotowa.

2. Z komputera administracyjnego spróbuj wykonać zdalne zapytanie, np. przy użyciu „Test-WsMan" lub uruchamiając zdalną sesję PowerShell (w zależności od używanego narzędzia).

9. Podsumowanie

Zastosowanie GPO do włączenia PowerShell Remoting (WinRM) na stacjach roboczych Windows 10 / 11 zapewnia spójne, centralnie zarządzane środowisko do zdalnej administracji. Po prawidłowym skonfigurowaniu ustawień WinRM oraz reguł zapory, administrator może wykonywać zdalne komendy i skrypty PowerShell na wielu komputerach jednocześnie, bez ręcznej konfiguracji każdego hosta.