Konfiguracja oprogramowania

- Konfiguracja kont MSA / gMSA
- Konfiguracja WinRM - Zarządzanie zdalne systemem operacyjnym

Konfiguracja kont MSA / gMSA

Na kontrolerze domeny:

Logujemy się na konto w domenie w której chcemy użyć kont gMSA,
Używamy aplikację PowerShell by sprawdzić wersję domeny:

```
(Get-ADDomain).ForestMode
(Get-ADDomain).DomainMode
```

A black background with white textAI-generated content may be incorrect.

Dodajmy główny klucz KDS - Ustawiamy -10 godzin by automatycznie zresetować jego długość życia:

```
Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
```

A computer screen with white textAI-generated content may be incorrect.

Testujemy poprawność klucza:

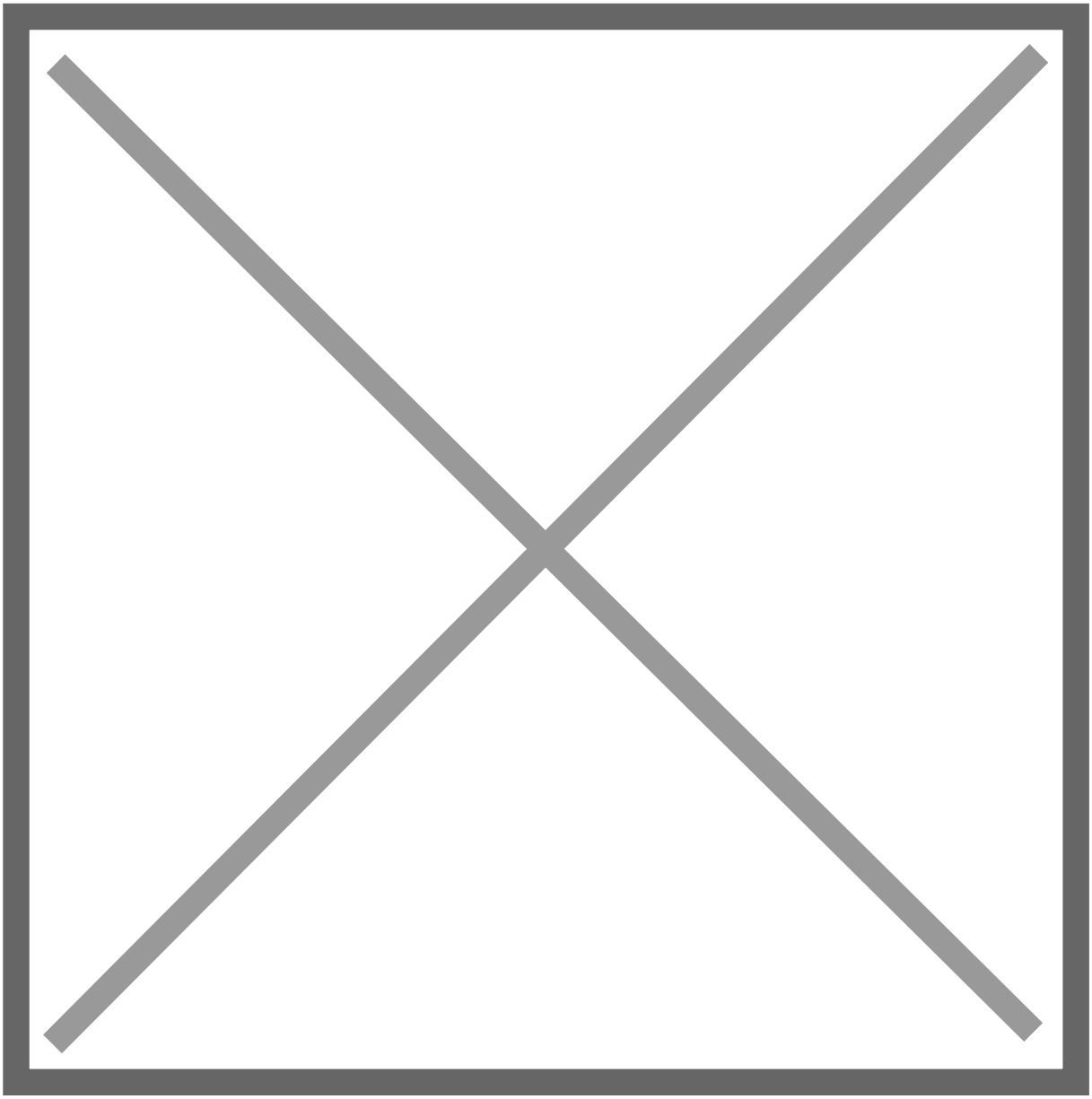
```
Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId
```

A black screen with white textAI-generated content may be incorrect.

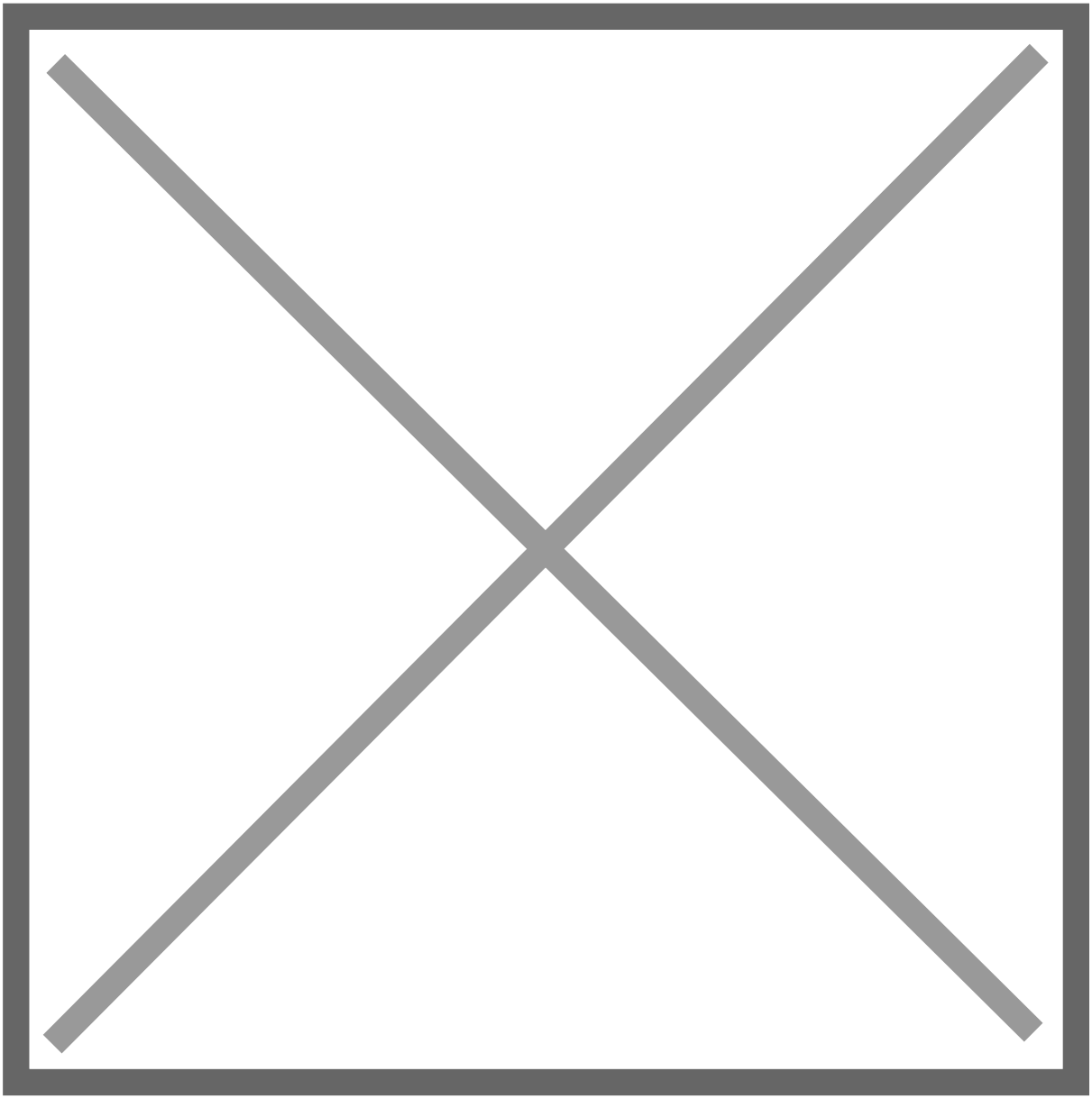
Dodajemy odpowiednie konto:

Ważne Częstotliwość automatycznej zmiany haseł można podać tylko przy tworzeniu konta, domyślnie jest 30dni

```
New-ADServiceAccount -Name NazwaKonta -DNSHostName NazwaKonta.AktualnaDomena -
ManagedPasswordIntervalInDays LiczbaDni
```



Dla przykładu:

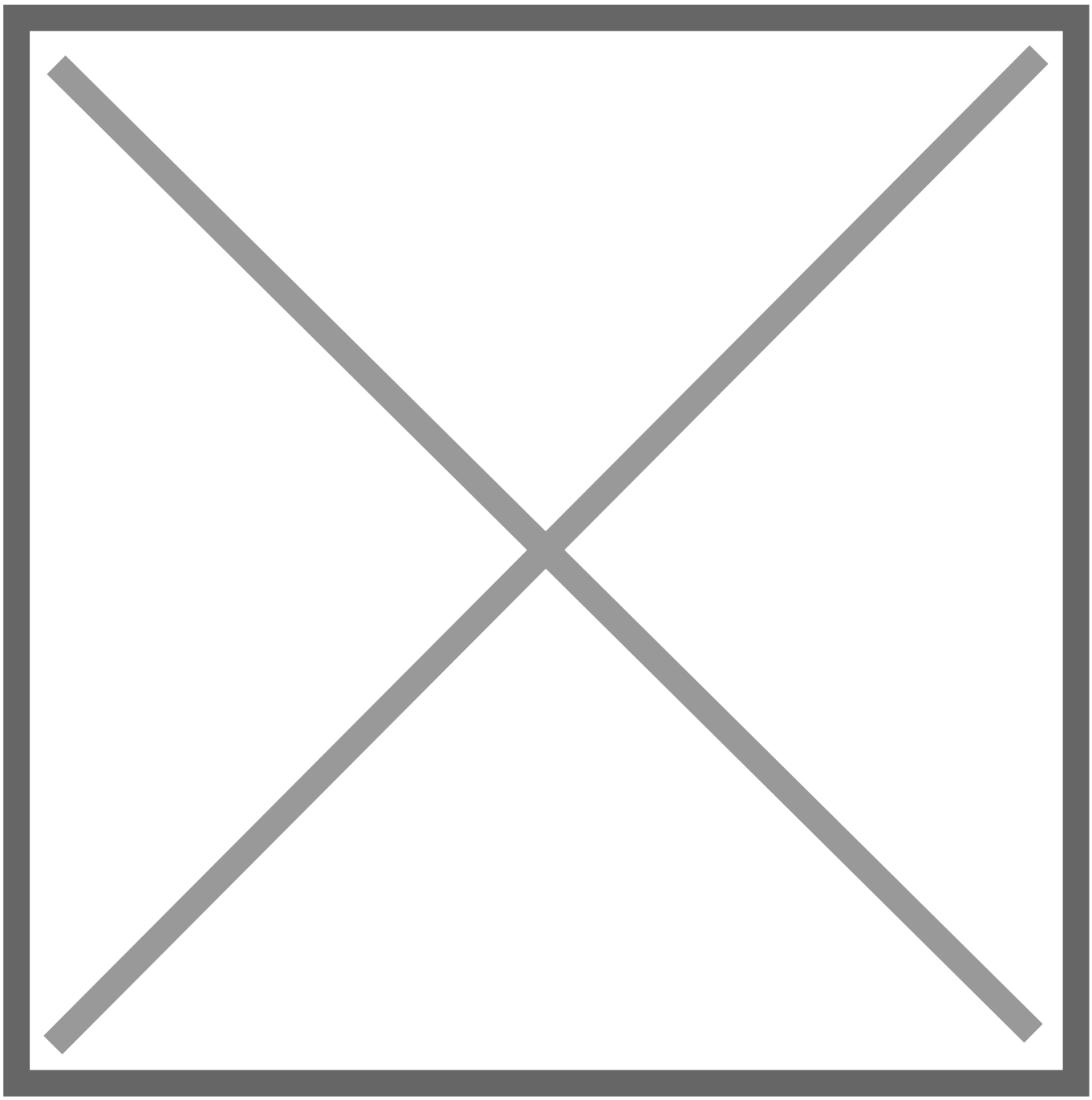


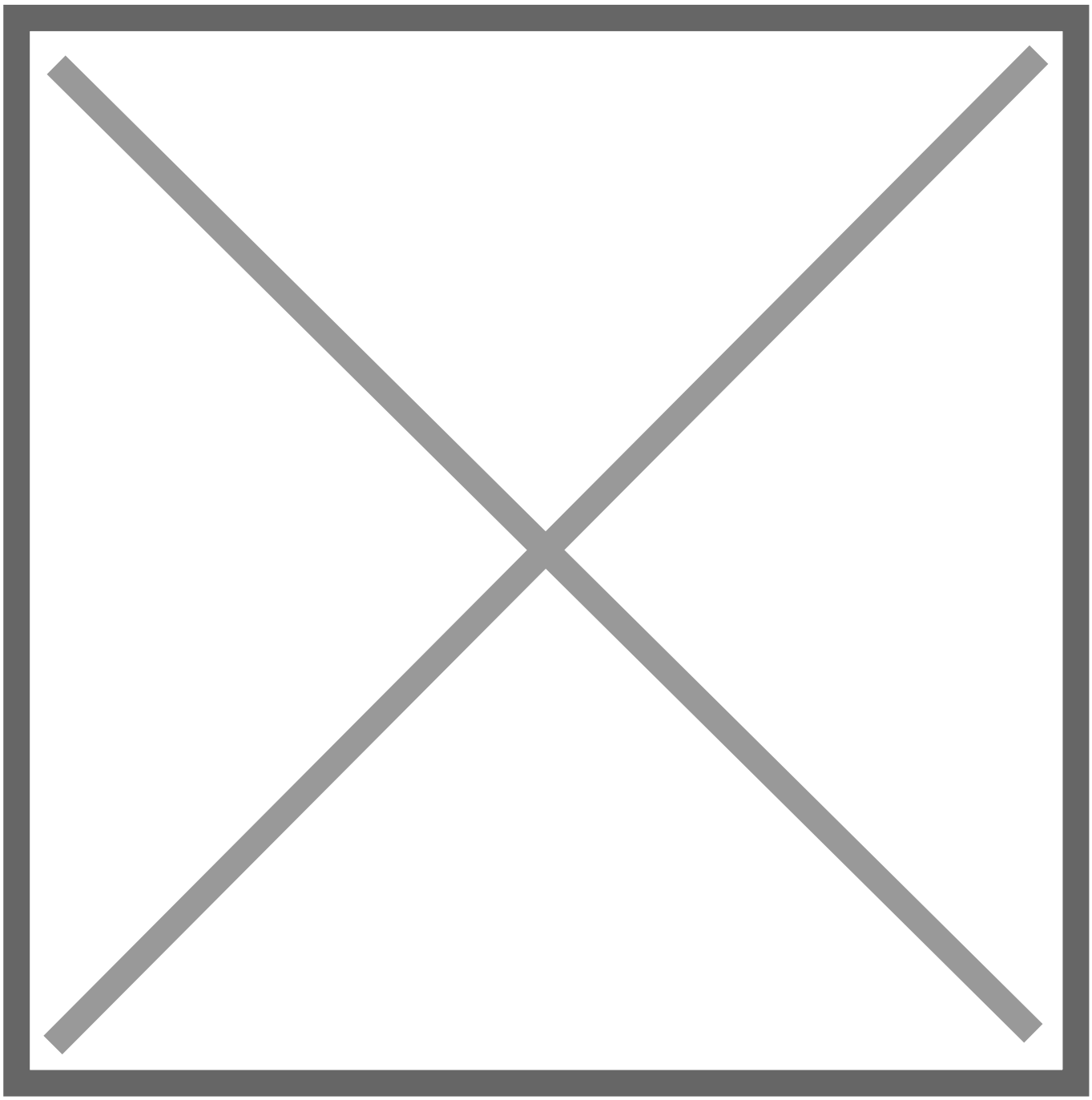
A screenshot of a computerAI-generated content may be incorrect.

Dodajemy grupę która może zarządzać danym kontem i do niej **konto komputera** które może skorzystać z naszego konta gMSA

A screenshot of a computer screenAI-generated content may be incorrect.

```
Set-ADServiceAccount -Identity "NazwaKonta" -PrincipalsAllowedToRetrieveManagedPassword "NazwaGrupy"
```





Na serwerze docelowym:

Najpierw musimy zainstalować przystawki powershell do zarządzania AD:

```
Add-WindowsFeature RSAT-AD-PowerShell
```

A screen shot of a computerAI-generated content may be incorrect.

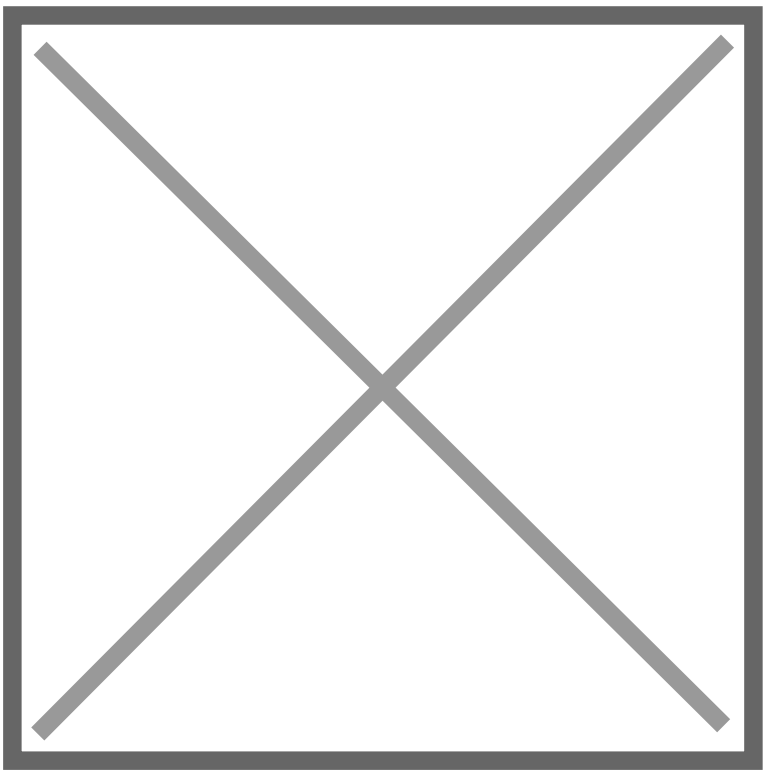
Resetujemy ticket autentykacji Kerberos:

```
klist purge -li 0x3e7
```

A screen shot of a computer codeAI-generated content may be incorrect.

I instalujemy konto:

```
Install-ADServiceAccount -Identity "NazwaKonta"
```



Przykładowy wynik:

A screen shot of a computerAI-generated content may be incorrect.

I weryfikujemy instalację:

```
Test-ADServiceAccount -Identity NazwaKonta
```

A black background with white textAI-generated content may be incorrect.

Po tych akcjach konto jest dostępne:

A screenshot of a computerAI-generated content may be incorrect.

A screenshot of a computerAI-generated content may be incorrect.

Na podstawie:

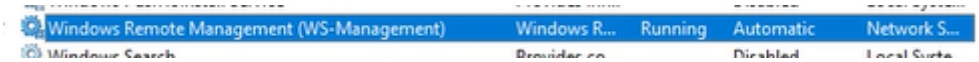
Secure group managed service accounts - Microsoft Entra | Microsoft Learn

Konfiguracja WinRM - Zarządzanie zdalne systemem operacyjnym

Sprawdzenie działania usług

Do zdalnego zarządzania systemem operacyjnym muszą być uruchomione usługi:

WinRM



Przepuszczenie ruchu sieciowego:

By można było się połączyć do danej maszyny, musimy przepuścić ruch po porcie 445 + 139 oraz warto też od razu dodać ping:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow -Profile Any


netsh advfirewall firewall add rule name="Open Port 139 - SMB over NetBIOS" dir=in action=allow protocol=TCP localport=139
netsh advfirewall firewall add rule name="Open Port 445 - SMB" dir=in action=allow protocol=TCP localport=445
```

Problem "Access Denied (5)"

Dodatkwo, w razie problemów z "Access Denied (5)", należy zweryfikować wpis w rejestrze:

```
$newItemPropertySplat = @{
  Name = 'LocalAccountTokenFilterPolicy'
  Path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
  PropertyType = 'DWord'
  Value = 1
}
```

```
New-ItemProperty @newItemPropertySplat
```