

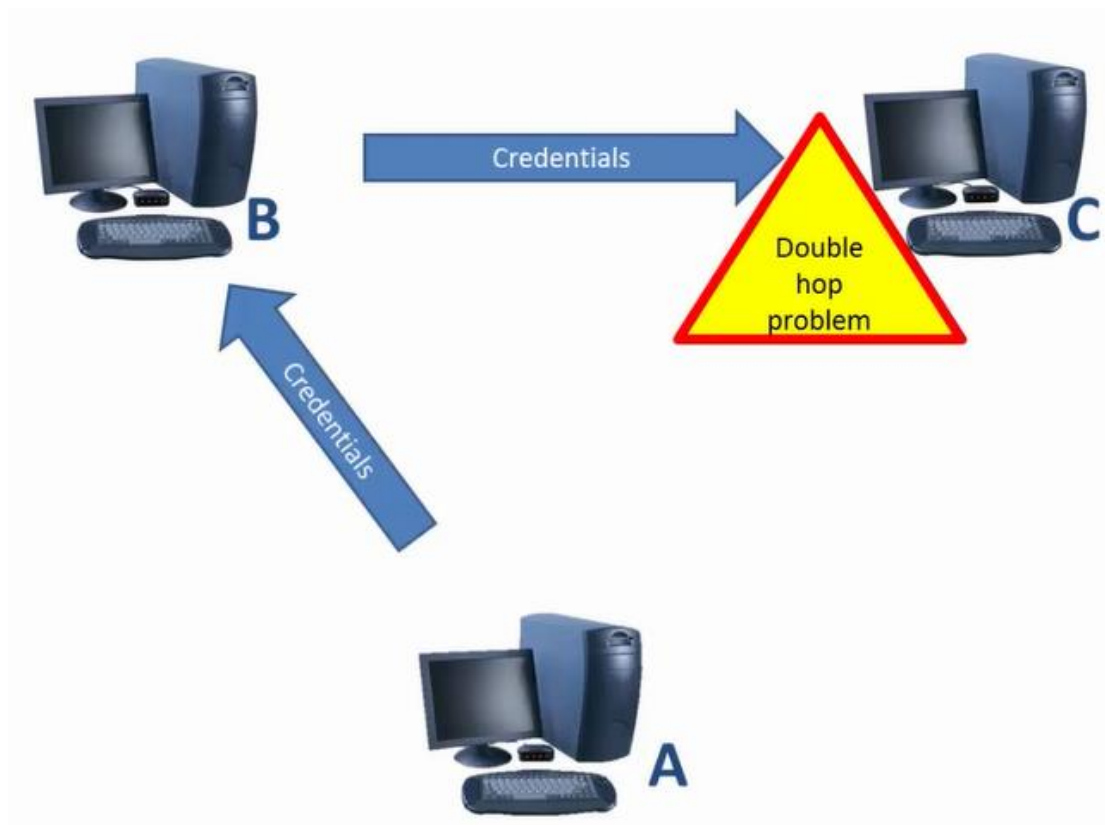
Przekazywanie poświadczeń między serwerami - info

Omówienie scenariusza tzw. Double Hop

Konfiguracja serwera pośredniczącego w przekazywaniu poświadczeń

Konfiguracja komputera lokalnego

Konfiguracja komputerów za pomocą zasad grupy



Użytkownik jest zalogowany na A i zleca z udziałem remotingu wykonanie zadania na B, polecenie wykonywane na komputerze B musi sięgnąć do pewnych zasobów komputera C, po drodze należy przekazywać poświadczenia użytkownika z A do B a następnie z B do C. Taki scenariusz nie zadziała, ta sytuacja to **Double hop problem**.

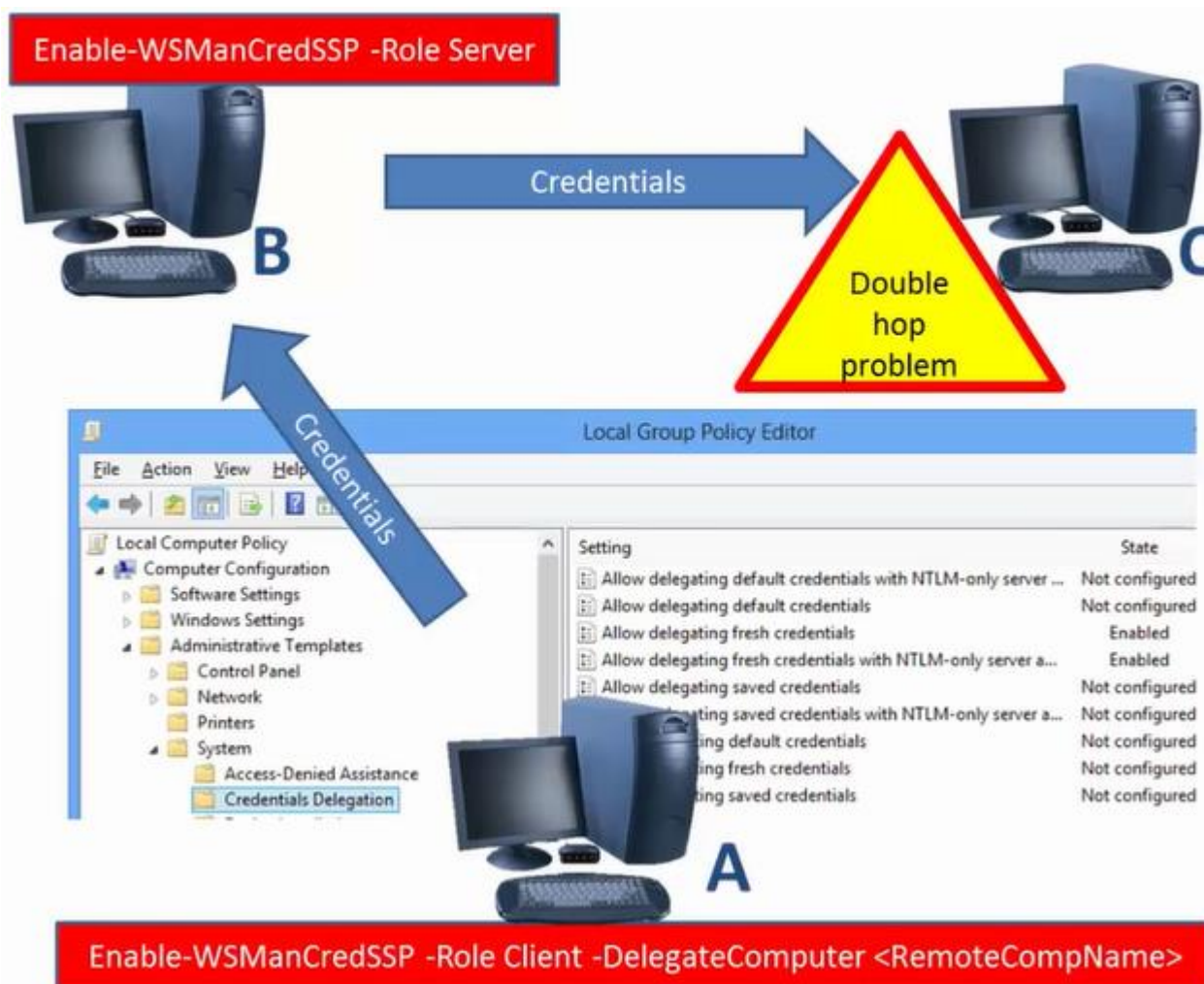
B nie ma prawa przekazywać otrzymane poświadczenia z A do C w tym wypadku a w ogóle gdziekolwiek dalej.

W konfiguracji remoutingu można zezwolić na dalsze przekazywanie poświadczeń z B do C, odpowiednia konfiguracja dotyczy A i B.

Na B musi być włączona obsługa protokołu **CredSSP** dzięki temu otrzymane poświadczenia będzie można przekazywać dalej.

Na komputerze A należy zezwolić, aby poświadczenia wprowadzone na A mogły być przekazywane dalej do B korzystając z opcji **DelegateComputer**, określasz tu wyraźnie które komputery będą

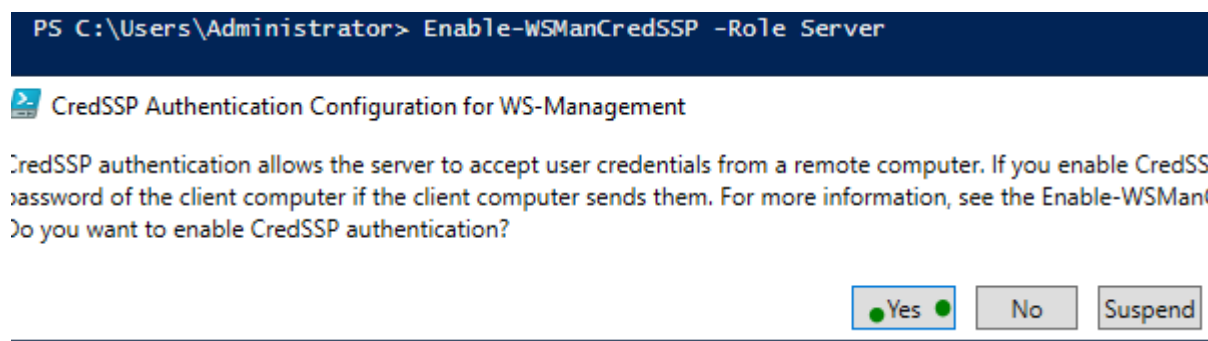
upoważnione do przesyłania poświadczeń dalej. U mnie powinien tu być wymieniony B.
Zmiany można wymuszać także za pomocą zasad grupy za pomocą włączenia opcji **Allow delegating fresh credentials**



W przypadku **Duble hop problem** należy wykonać dodatkowo konfigurację serwera (komputera) który stanie się uprawniony do przekazywania poświadczeń użytkownika

Polecenie poniższe włącza rolę komputera pośredniczącego, pozwalamy na to, aby otrzymane poświadczenie było przekazywane dalej do innego serwera, jeżeli zajdzie taka potrzeba.

Komendę należy uruchomić na komputerze, który konfigurujemy w roli komputera pośredniczącego.



```
PS C:\Users\Administrator> Enable-WSManCredSSP -Role Server

cfg           : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
lang          : pl-PL
Basic         : false
Kerberos      : true
Negotiate     : true
Certificate   : false
CredSSP       : true
CbtHardeningLevel : Relaxed
```

To nie wszystko.

Kolejne polecenie konfiguruje komputer lokalny

Ne może być tak aby serwer zdalny przekazywał wszystkie otrzymane od klientów poświadczenia bez zgody tych klientów, klienci muszą być świadomi, że serwer, do którego przekazują poświadczenia jest uprawniony do przekazywania ich dalej. Tutaj definiujemy, że komputer lokalny będzie w scenariuszu **Duble hop** pełnił funkcje klienta i wysyłając poświadczenia do komputera zdalnego serwer pozwala, aby serwer poświadczenia przekazywał dalej.

```
PS C:\Users\Administrator> Enable-WSManCredSSP -Role Client -DelegateComputer server
```

 CredSSP Authentication Configuration for WS-Management

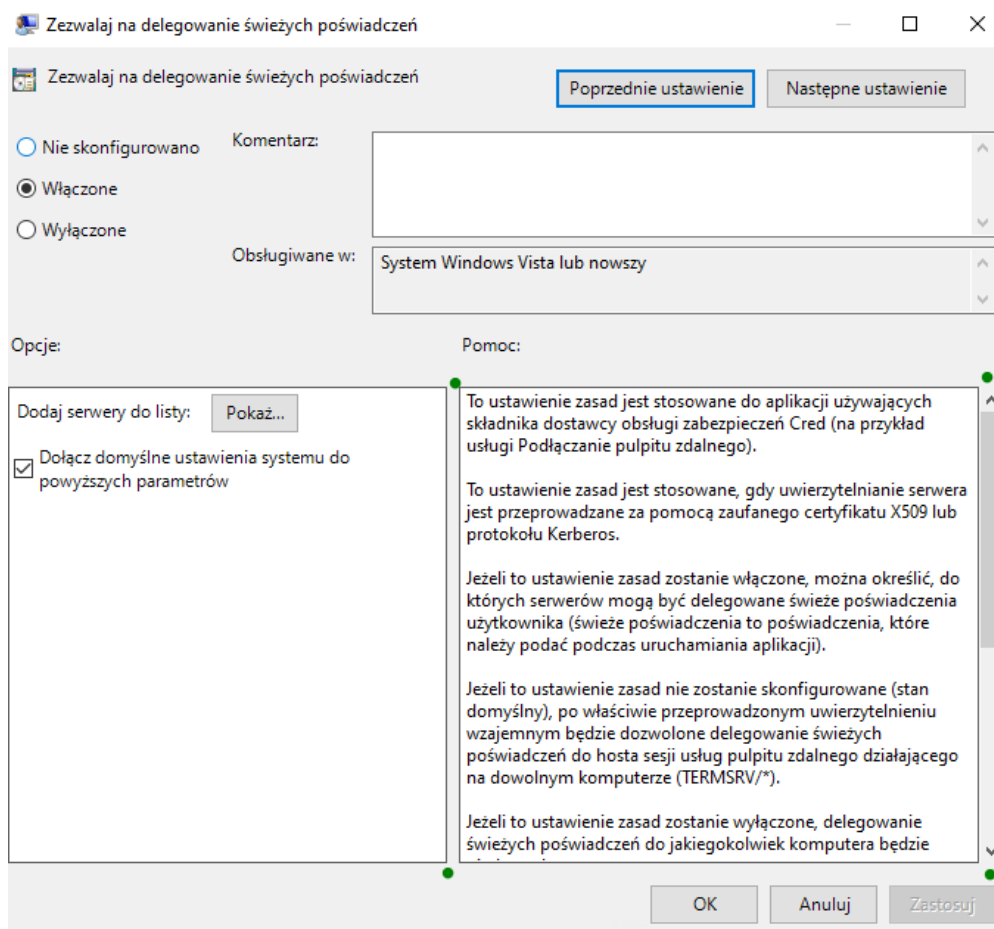
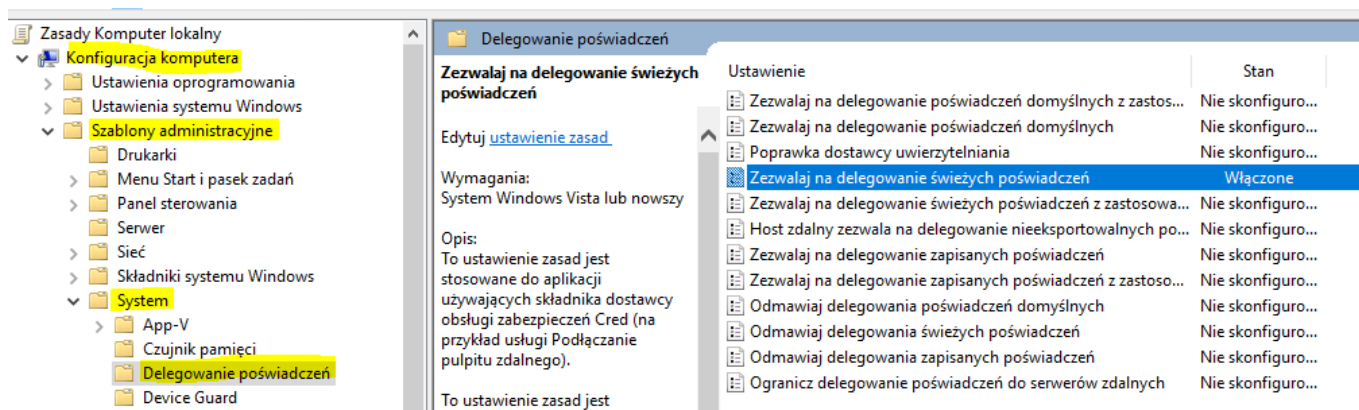
CredSSP authentication allows the user credentials on this computer to be sent to a remote computer. If you use CredSSP authentication for computer, that computer will have access to your user name and password. For more information, see the Enable-WSManCredSSP Help topic. Do you want to enable CredSSP authentication?

```
PS C:\Users\Administrator> Enable-WSManCredSSP -Role Client -DelegateComputer server

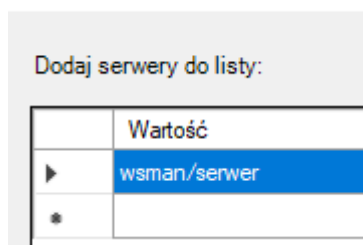
cfg           : http://schemas.microsoft.com/wbem/wsman/1/config/client/auth
lang          : pl-PL
Basic         : true
Digest       : true
Kerberos      : true
Negotiate     : true
Certificate   : true
CredSSP       : true
```

Komputer kliencki pozwala na przekazywanie poświadczeń tylko przez komputer o nazwie serwer a inne komputery nie będą mogły przesyłać poświadczeń dalej.

Do roli serwera pośredniczącego należy wybierać tylko najlepiej zabezpieczone maszyny, atak przeprowadzony na taki system pozwala na przechwytywanie poświadczeń wysoko uprzywilejowanych użytkowników, wymienione tu ustawienia mogą być również zmienione przez ustawienia zasady grup w domenie lub indywidualnie na komputerze w lokalnych zasadach zabezpieczeń.



Pokaż zawartość



Konfiguracja pozwala na wybór protokołów, nazw serwerów, do których można dalej przekazywać poświadczenia

Omówienie scenariusza tzw. Double Hop

Konfiguracja serwera pośredniczącego w przekazywaniu poświadczeń

Konfiguracja komputera lokalnego

Konfiguracja komputerów za pomocą zasad grupy