Cw47 Zbieranie zdarzeń

W tym ćwiczeniu skonfigurujemy komputer z 10-ką do przekazywania zdarzeń do kontrolera domeny ROL.

Podgląd zdarzeń umożliwia przeglądanie zdarzeń i dzienników na komputerze. Rozwiązanie problemu może wymagać wyświetlenia plików dziennika z innych zdalnych komputerów. Subskrypcja dziennika zdarzeń wchodzi w grę. Subskrypcja umożliwia zapisywanie zdarzeń ze zdalnych komputerów.
W tym artykule zamierzam skonfigurować kolektor i system docelowy.

Załóżmy, że chcesz zbierać zdarzenia dziennika zdarzeń z kontrolera domeny na komputerze klienckim. Dlatego komputer kliencki jest kolektorem, a kontroler domeny jest celem.

Ćwiczenie 1 Konfigurowanie komputera do zbierania zdarzeń

W tym ćwiczeniu skonfigurujesz komputer ROL do zbierania zdarzeń,
1. Zaloguj się do ROL przy użyciu konta domenowego z administracyjnymi uprawnieniami.
2. W wierszu polecenia uruchom polecenie do konfigurowania usługi kolektor zdarzeń systemu Windows:

wecutil qc

Gdy pojawi się monit o zmianę trybu startu usługi na Opóźniony start, Wpisz T i wciśnij Enter.

Ćwiczenie 2 Konfigurowanie komputera do przekazywania zdarzeń

W tym ćwiczeniu skonfigurujesz komputer z 10-ką do przekazywania zdarzeń do zbierającego komputera.
Przed wykonaniem tego ćwiczenia należy zrobić Ćwiczenie 1.
Zaloguj się na komputer z 10-ką, używając konta domeny z uprawnieniami administracyjnymi.
W wierszu pomiecenia uruchom następujące polecenie do skonfigurowanie usługi Zdalne zarządzanie Windows:

winrm quickconfig

Gdy pojawi się monit o zmianę trybu uruchamiania usługi, utworzenie odbiornika usługi WinRM i włączenie wyjątku zapory, wpisz Y i wciśnij Enter.

Komputer serwera (system docelowy)

Sprawdź, czy usługa Zdalne zarzadzanie systemem Windows (Windows Remote Management) jest skonfigurowana do automatycznego uruchamiania przez wybór węzła Usługi (Services), wybranie usługi Windows Remote Management (WS-Management) (Zdalne zarzadzanie systemem Windows (WS-

Management)) i weryfikację, że jest uruchomiona, a Typ uruchomienia (Startup Type) to Automatyczne (opóźnione uruchomienie) (Automatic (Delayed Start)).

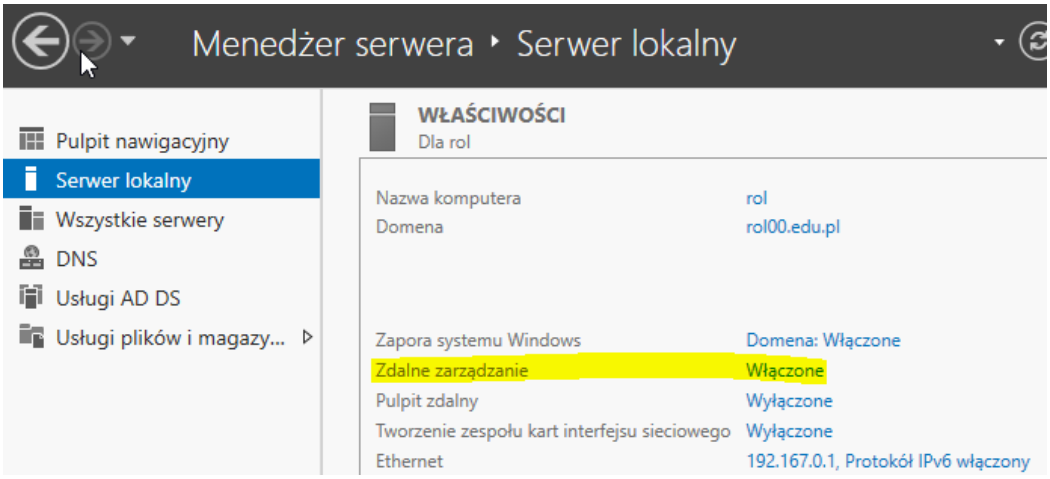
W systemach Windows Server 2012 i 2016 Zdalne zarządzanie jest domyślnie włączone. Aby się upewnić, że jest włączony, wpisz

Configure-SMRemoting.exe -GET

Jeśli Remoting nie jest włączony, możesz go po prostu włączyć, uruchamiając

Configure-SMRemoting.exe -ENABLE

Zanim przejdziemy do następnego kroku, otwórz Menedżera serwera i upewnij się, że Zdalne zarządzanie jest ustawione na Włączone.



Teraz musimy dodać konto komputera kolekcjonera do grupy czytników dzienników zdarzeń serwera. Możesz to zrobić w cmd lub PowerShell.

Uruchom następujące polecenie w wierszu polecenia, aby przyznać dostęp de do dziennika zdarzeń.

Jeżeli komputer zbierający ma inną nazwę lub nazwę domeny, zastąp de prawidłową nazwą komputera, a rol00.edu.pl prawidłową nazwą domeny.
de – w tym przypadku nazwa komputera z Windows 10 – wpisz własną

net localgroup "Event Log Readers" rol00.edu.pl\de$ /add

```
C:\Users\Administrator>net localgroup "Użytkownicy dzienników wydajności" rol00.edu.pl\de$ /add
Polecenie zostało wykonane pomyślnie.
```

Lub w PowerShell

Add-ADGroupMember -Identity "Event Log Readers" -Members "de$

W celu sprawdzenia:

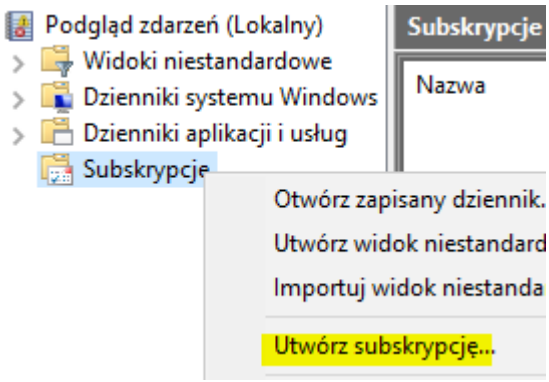
```
C:\Users\Administrator>net localgroup "Użytkownicy dzienników wydajności"
Nazwa aliasu     Użytkownicy dzienników wydajności
Komentarz        Członkowie tej grupy mogą planować rejestrowanie liczników
ierać wyniki śledzenia zdarzeń, zarówno lokalnie, jak i za pomocą dostępu zd

Członkowie

-------------------------------------------------------------------------------
IS\de$
Polecenie zostało wykonane pomyślnie.
```

Ćwiczenie 3 Konfigurowanie subskrypcji zdarzeń

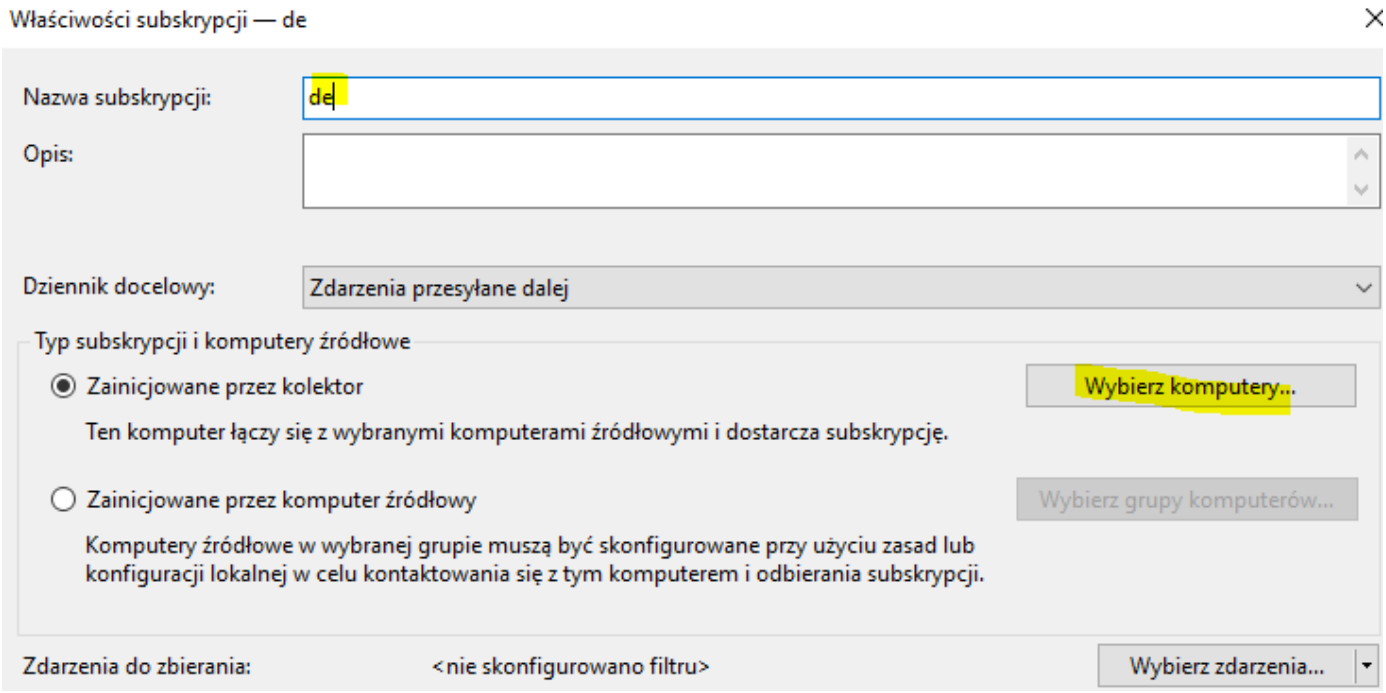
W tym ćwiczeniu utworzymy subskrypcje zdarzeń na ROL do zbierania zdarzeń z 10-ki.

Przed wykonaniem tego ćwiczenia należy ukończyć ćwiczenia 1 i 2.

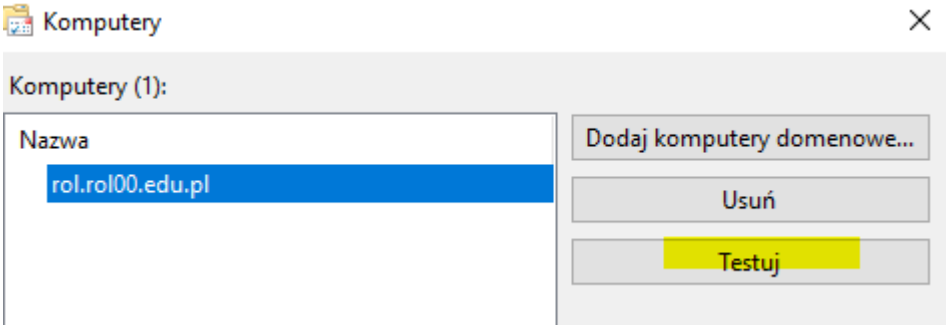
1. Zaloguj się do komputera kolekcjonera (Windows 10). Otwórz Podgląd zdarzeń (eventvwr). Kliknij Subskrypcje i wybierz Utwórz subskrypcję.

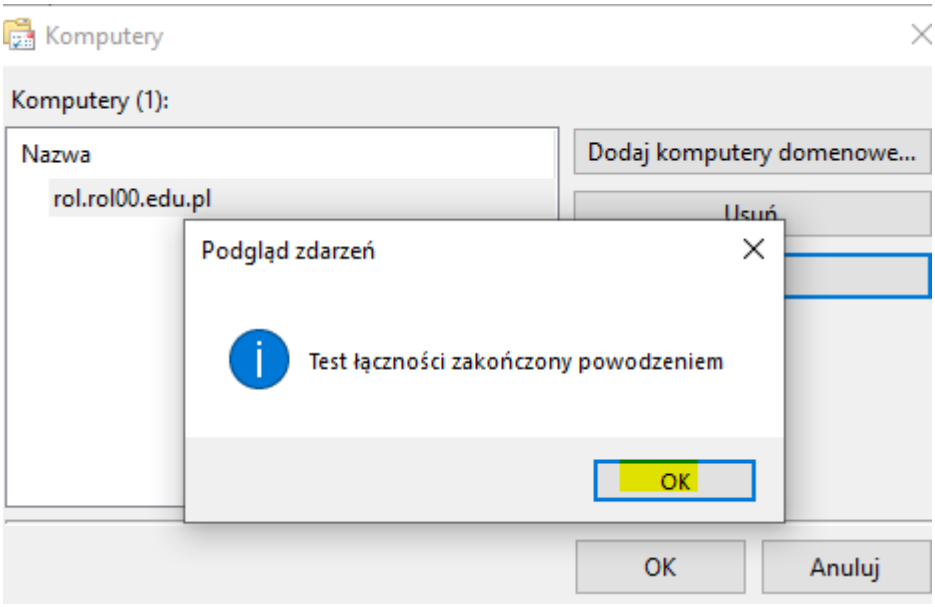


Wprowadź nazwę subskrypcji i kliknij Wybierz komputery.

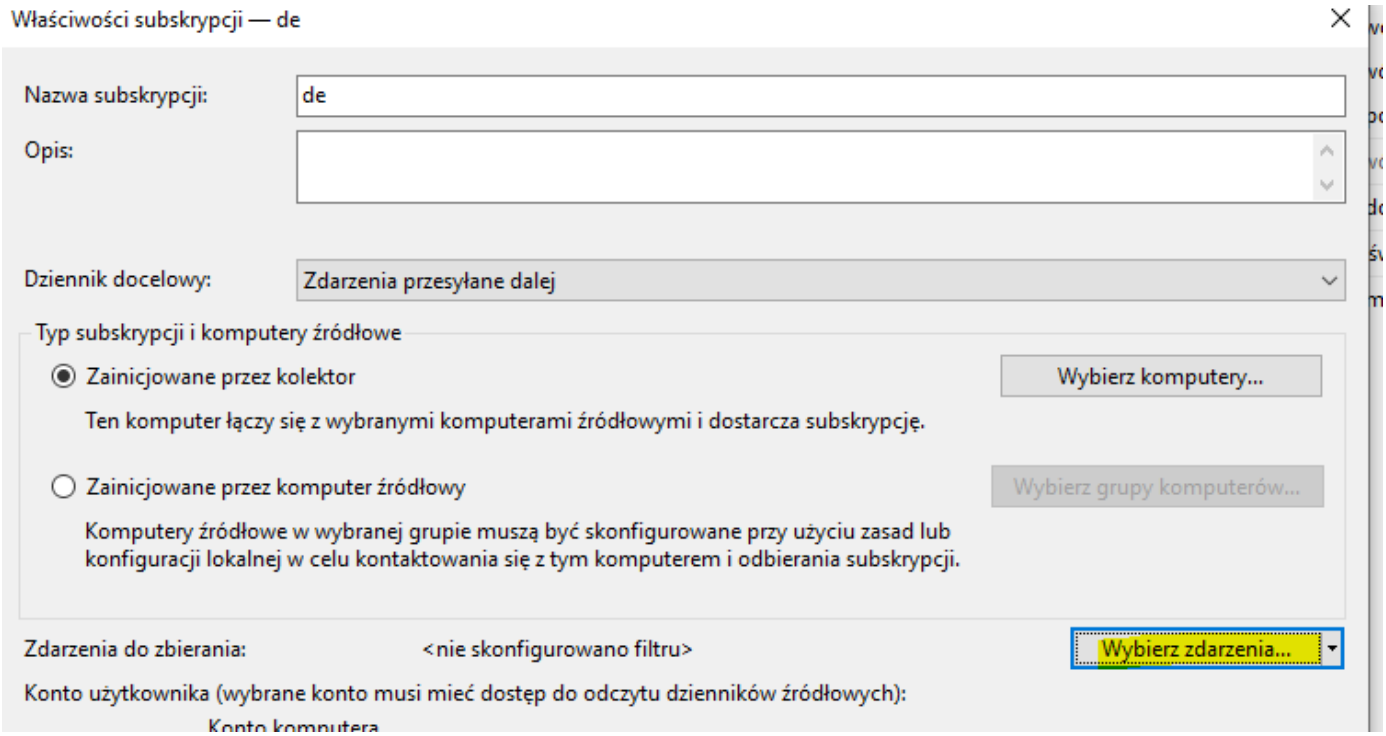


Kliknij Dodaj komputery domeny i wpisz nazwę komputera docelowego systemu. Przed kontynuowaniem warto przetestować połączenie.

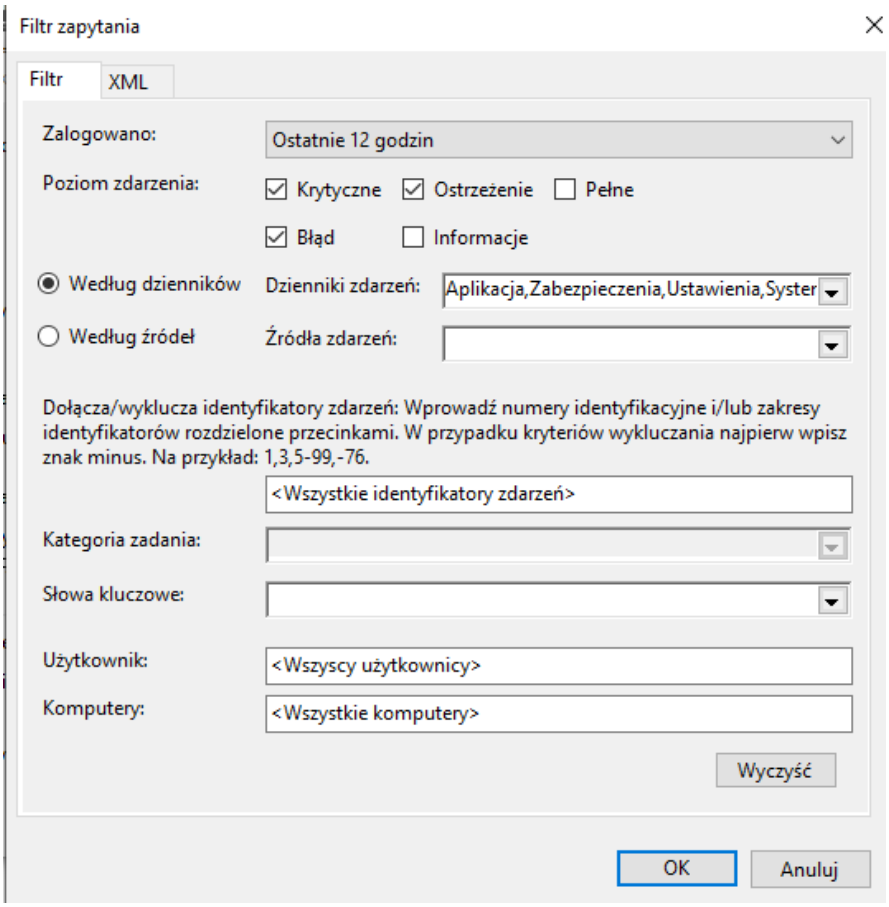




Zdefiniuj filtr zapytań. Wybierz wydarzenia, które chcesz zebrać.



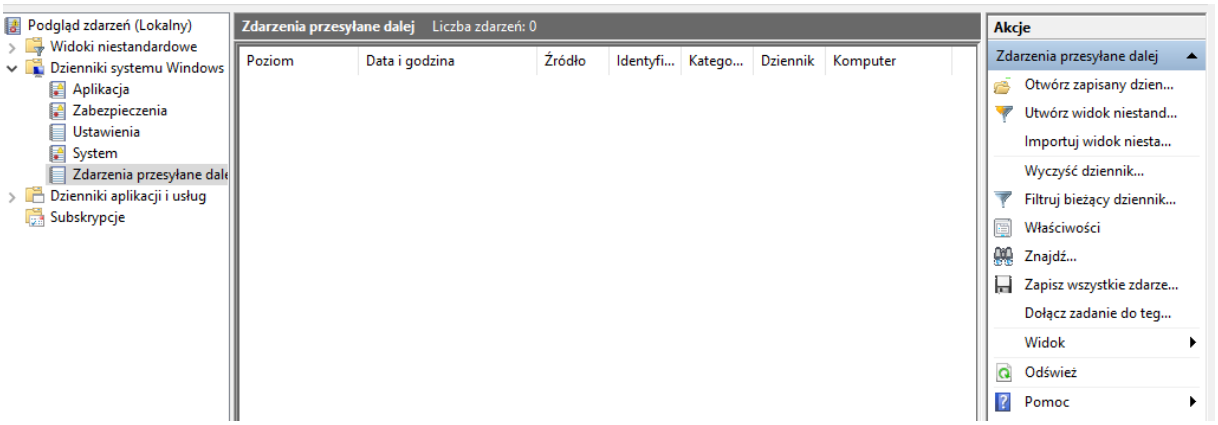
Zdefiniuj filtr zapytań. Wybierz wydarzenia, które chcesz zebrać.



Kliknij OK.

Testowanie subskrypcji dziennika zdarzeń

Poczekaj kilka minut i zrób coś w systemie docelowym. Na przykład ponownie uruchom komputer, aby uruchomić wpisy dziennika zdarzeń. Następnie wróć do systemu klienta i kliknij Dzienniki systemu Windows. Wybierz opcję Przekazywanie zdarzeń i przejrzyj dzienniki komputera docelowego.



Podsumowanie lekcji

Przekazywanie zdarzeń korzysta z HTTP lub HTTPS do wysyłania zdarzeń, które pasują do filtru, jaki się utworzy na zbierającym komputerze. Korzystając z przekazywania zdarzeń, można scentralizować zarzadzanie zdarzeniami i lepiej śledzić krytyczne zdarzenia, które odbywają się na komputerach klienckich i serwerach.

Przed przeprowadzeniem przekazywania zdarzeń musimy skonfigurować komputery zbierający i przekazujący. Na komputerze przekazującym, uruchamiamy polecenie winrm quickconfig.

Na zbierającym komputerze uruchamiamy polecenie wecutil qc. Następnie możemy skonfigurować subskrypcje zdarzeń na komputerze zbierającym.

Pytania do Iekcji

1. Administrator konfiguruje komputer o nazwie Server do zbierania danych z komputera o nazwie Client. Oba komputery są w domenie Rol00.edu.pl. Które z następujących poleceń uruchomi na komputerze zbierającym?

A. wecutil qc

B. winrm quickconfig

C. net localgroup ,,Event Log Readers" Server$@rol00.edu.pl /add

D. net localgroup ,,Event Log Readers" Client$@rol00.edu.pl /add

2. Administrator konfiguruje komputer o nazwie Server do zbierania zdarzeń z komputera o nazwie Client. Oba komputery znajdują się w domenie Rol00.edu.pl. Które z następujących poleceń uruchomi na komputerze przekazującym? (Podaj wszystkie prawidłowe odpowiedzi).

A. wecutil qc

B. winrm quickconfig

C. net localgroup ,,Event Log Readers" Server$@rol00.edu.pl /add

D. net localgroup ,,Event Log Readers" Client$@rol00.edu.pl /add

3. Administrator potrzebuje skonfigurować subskrypcje zdarzeń, aby aktualizowała się co minutę, Którego narzędzia użyje?

A. Wecutil

B. WinRM

C. Net

D. Konsoli Event Viewer