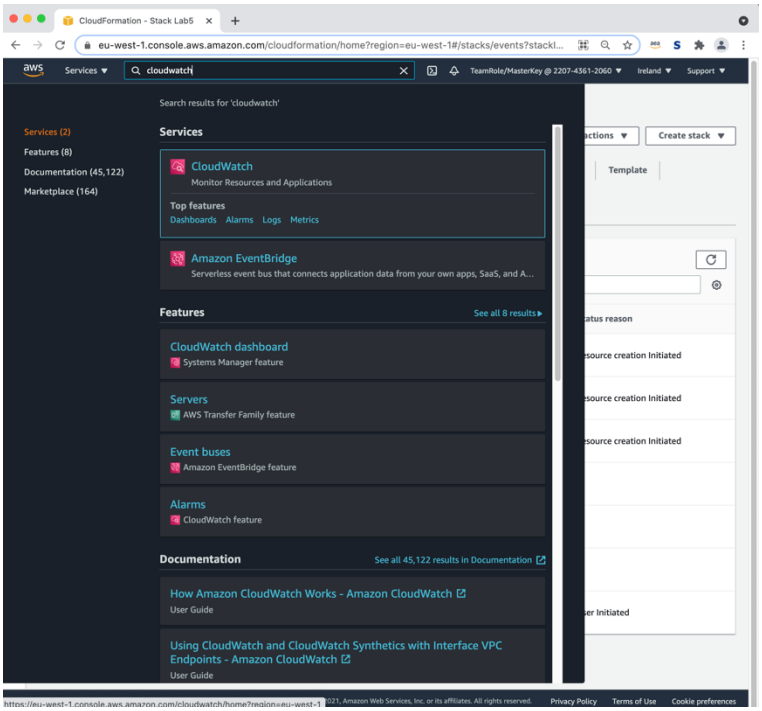
ĆWICZENIE NR 6

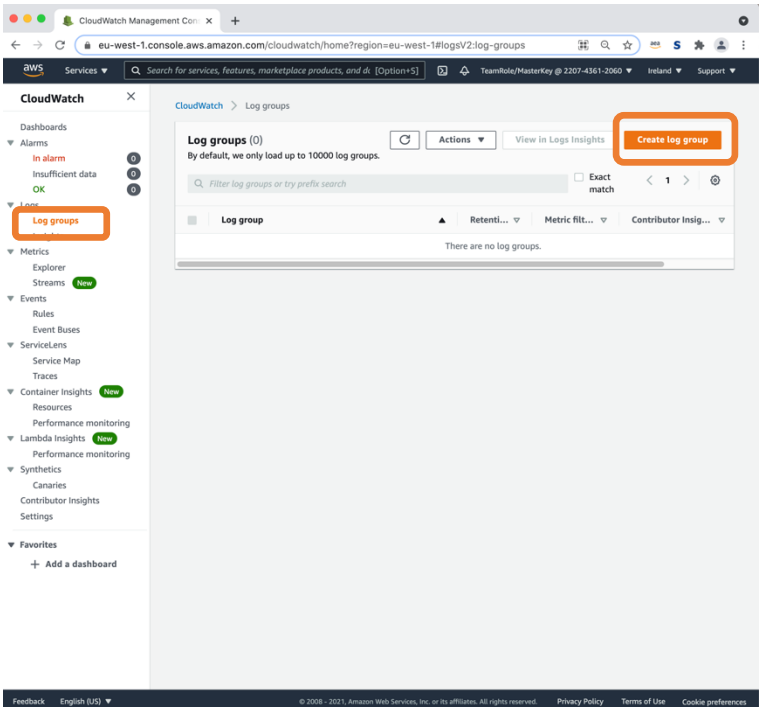
W tym ćwiczeniu korzystając z konfiguracji z ćwiczenia 5 podejrzymy co widać w logach.

1.1 Przygotuj log grupy dla VPC

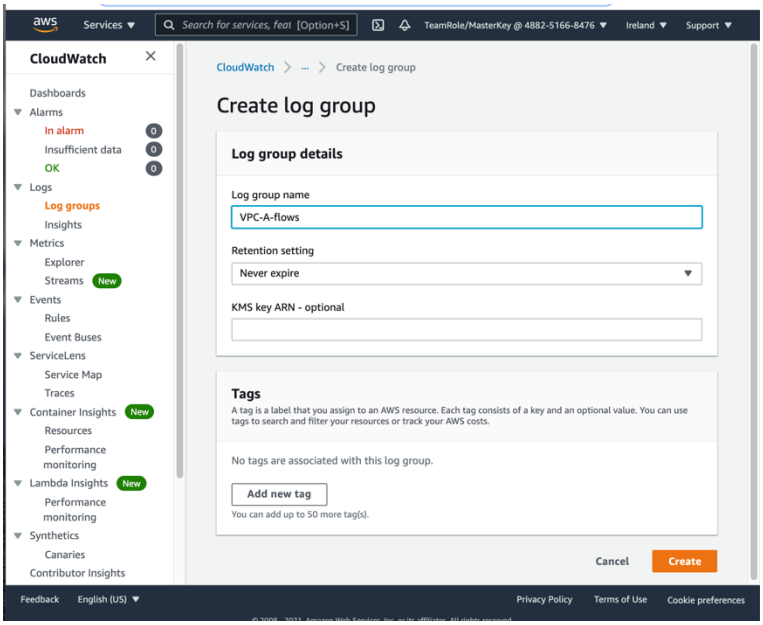
Wybierz stronę usługi CloudWatch.



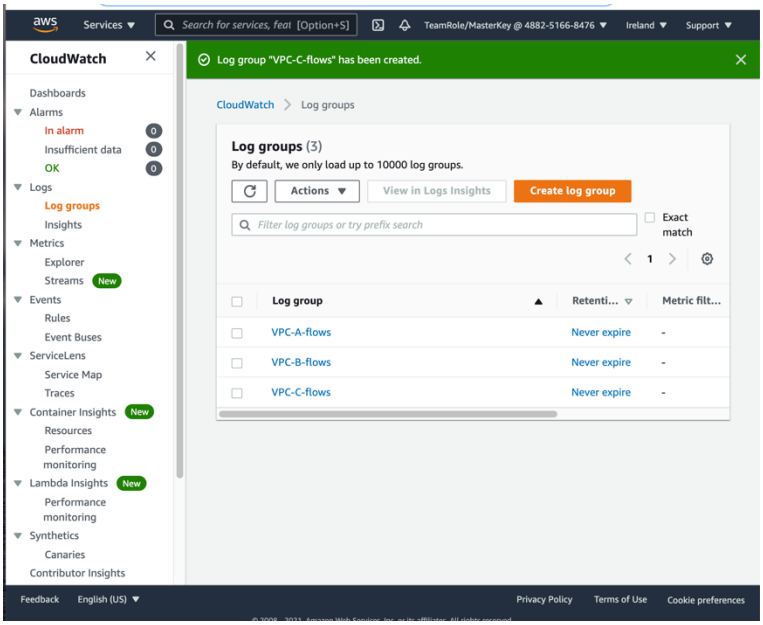
Z lewej strony z menu wybierz **Log groups**, a następnie **Create log group**.



Podaj nazwę grupy oraz retencję, domyślnie logi nie są usuwane. Efektem gromadzenia się dużych ilości logów jest opłata za ich przechowywanie.

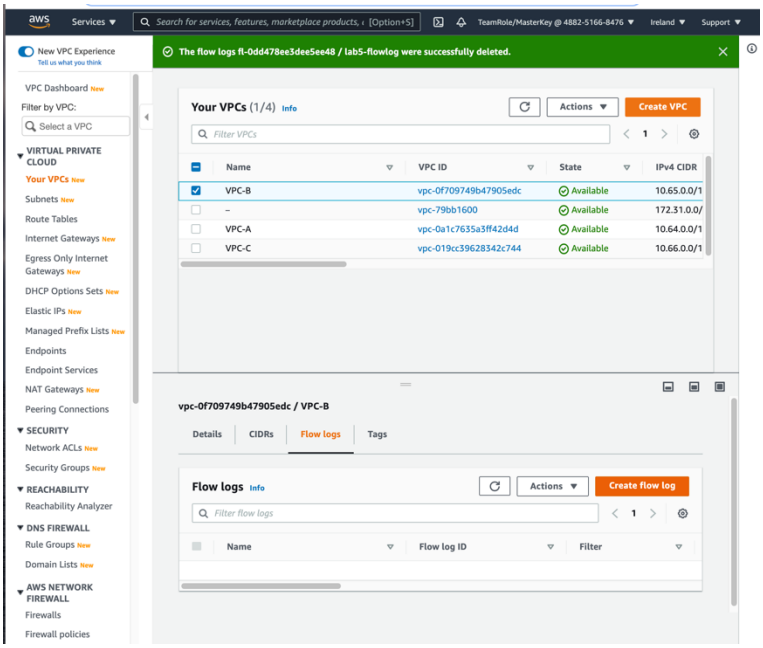


Do obserwacji różnych VPC rekomendowane jest definiowanie oddzielnych grup logujących (nie jest to wymagane).



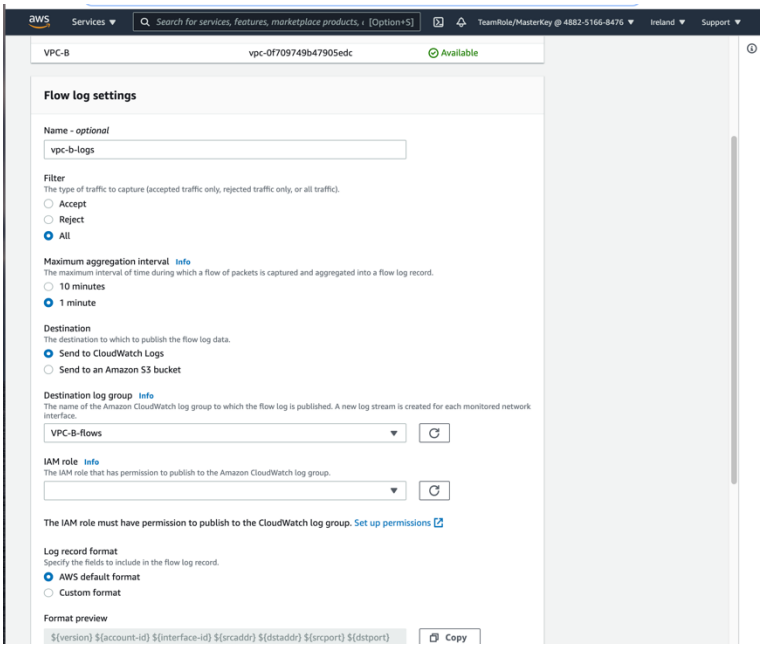
1.2 Włącz logowanie dla VPC

Ze strony usługi VPC wybierz **Your VPC** oraz zaznacz VPC-B, w zakładce **Flow logs** wybierz polecenie **Create flow log.**

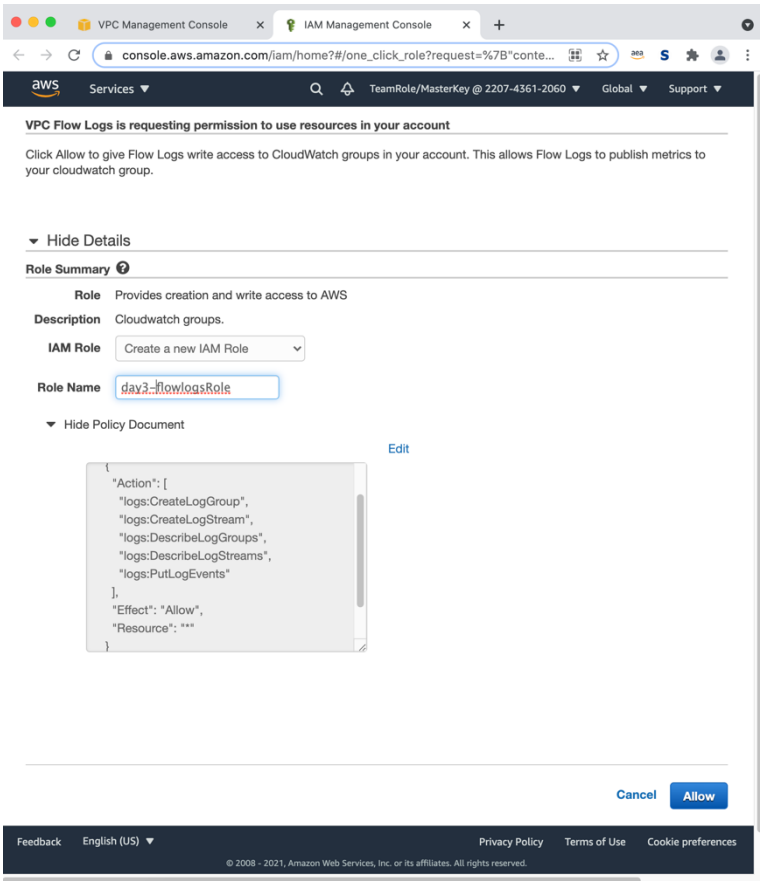


Podaj dane do konfiguracji logowania:

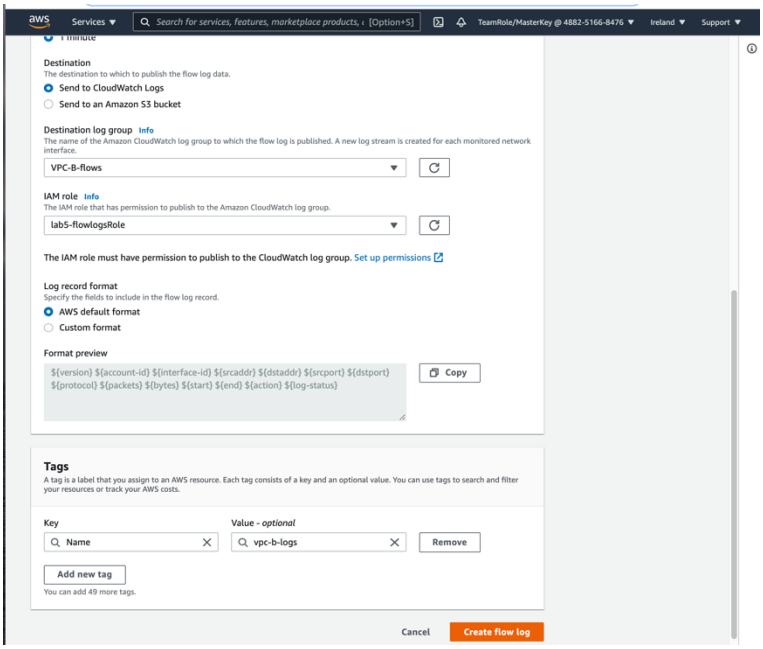
- Nazwa konfiguracji
- Filtrowanie – wybierz All
- Minimum aggregation interval – wybierz 1 minute
- Destination pozostaw CloudWatch i wybierz log grupę
- Otwórz link **Set up permissions**



W nowej zakładce nadaj proponowanej roli nazwę i zaakceptuj domyśle ustawienia.



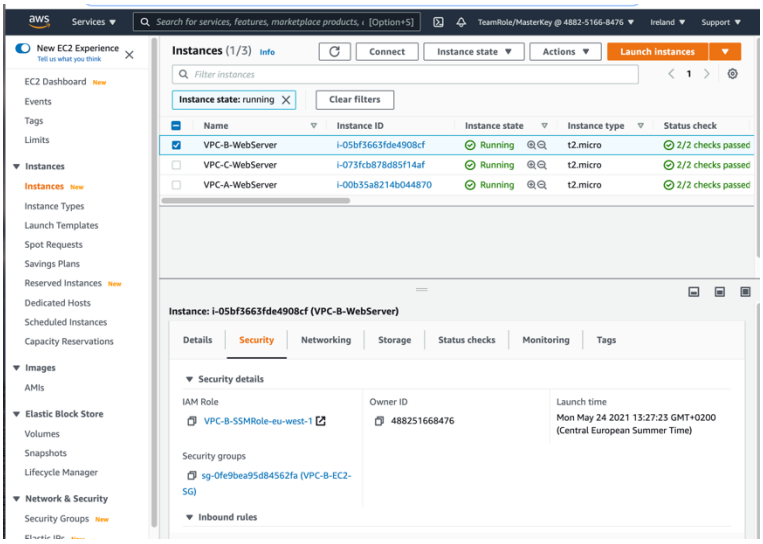
Odśwież wybór dla IAM role i wybierz rolę wcześniej przygotowaną w oddzielnej zakładce przeglądarki.



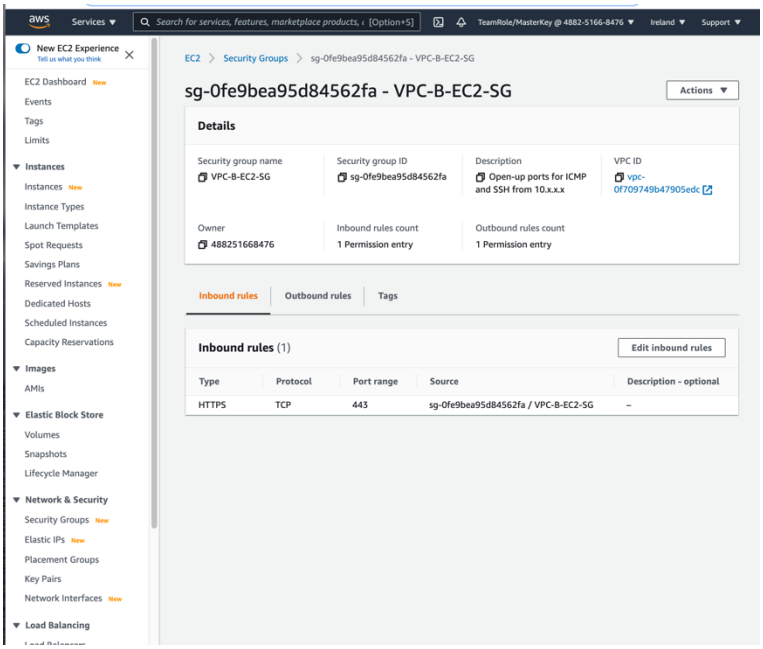
Zapisz konfigurację logowania. Możesz też ustawić logowanie w innych VPC.

1.3 Wygeneruj ruch sieciowy

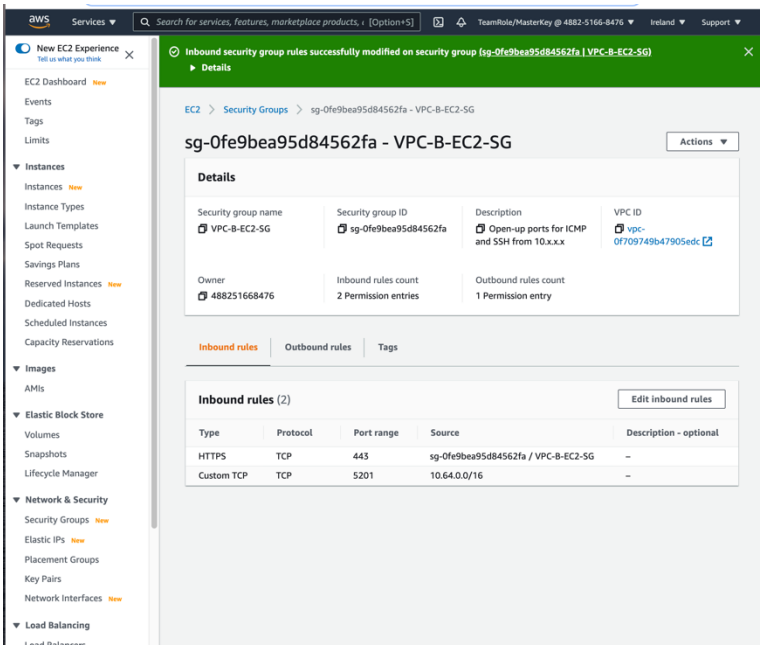
Wybierz serwer wirtualny z VPC-B oraz zakładkę **security** na stronie usługi EC2.



Otwórz stronę z konfiguracją **security group**.



Dodaj uprawnienia w security group do połączeń przychodzących z VPC-A na porcie 5201.

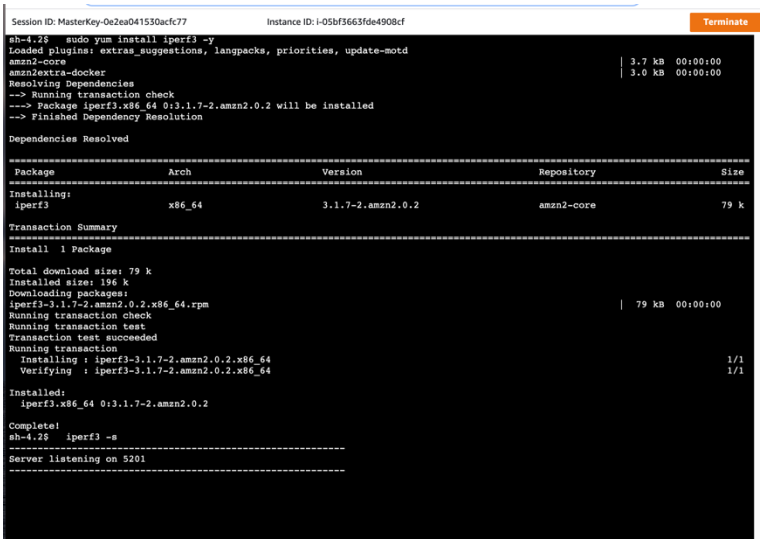


Połącz się z wykorzystaniem Session Manager do serwera z VPC-B i zainstaluj iperf3:

```
sudo yum install iperf3 -y
```

Uruchom:

```
iperf3 -s
```

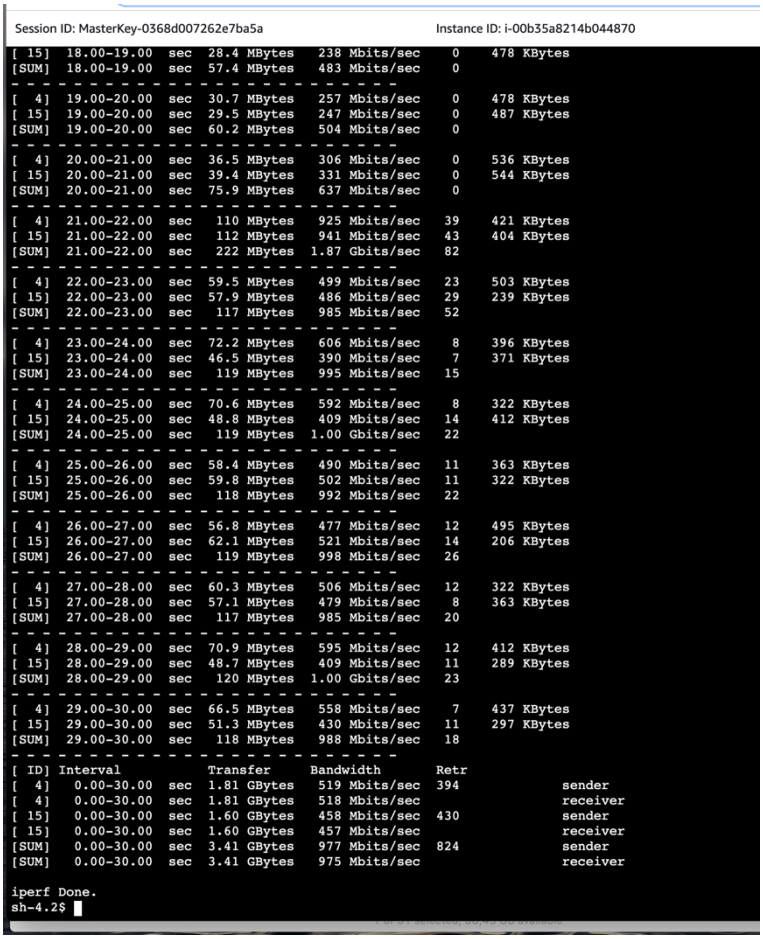


Teraz przygotuj konfigurację serwera w VPC-A. Odblokuj ACL, tak, aby możliwe było połączenie się do maszyny z Session Managera. Połącz się do maszyny i zainstaluj iperf3.

```
sudo yum install iperf3 -y
```

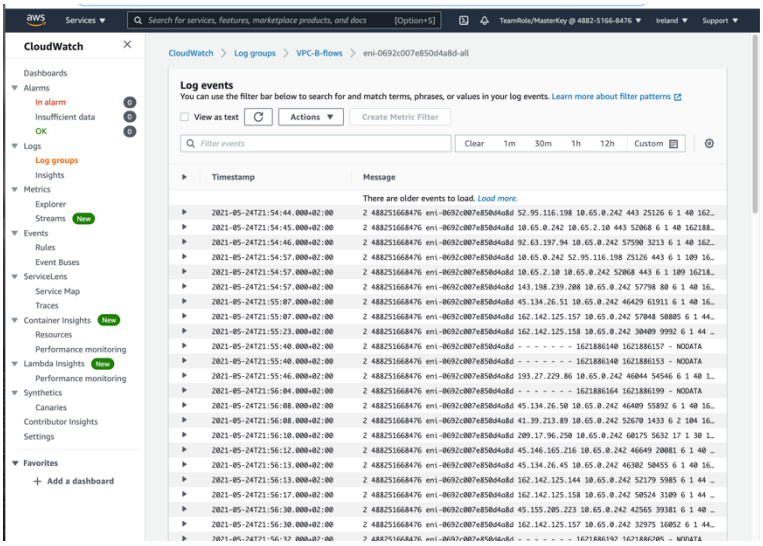
Uruchom transfer dwoma strumieniami przez 30 sekund do maszyny z VPC-B.

```
iperf3 -c 10.65.2.10 -P 2 -t 30
```



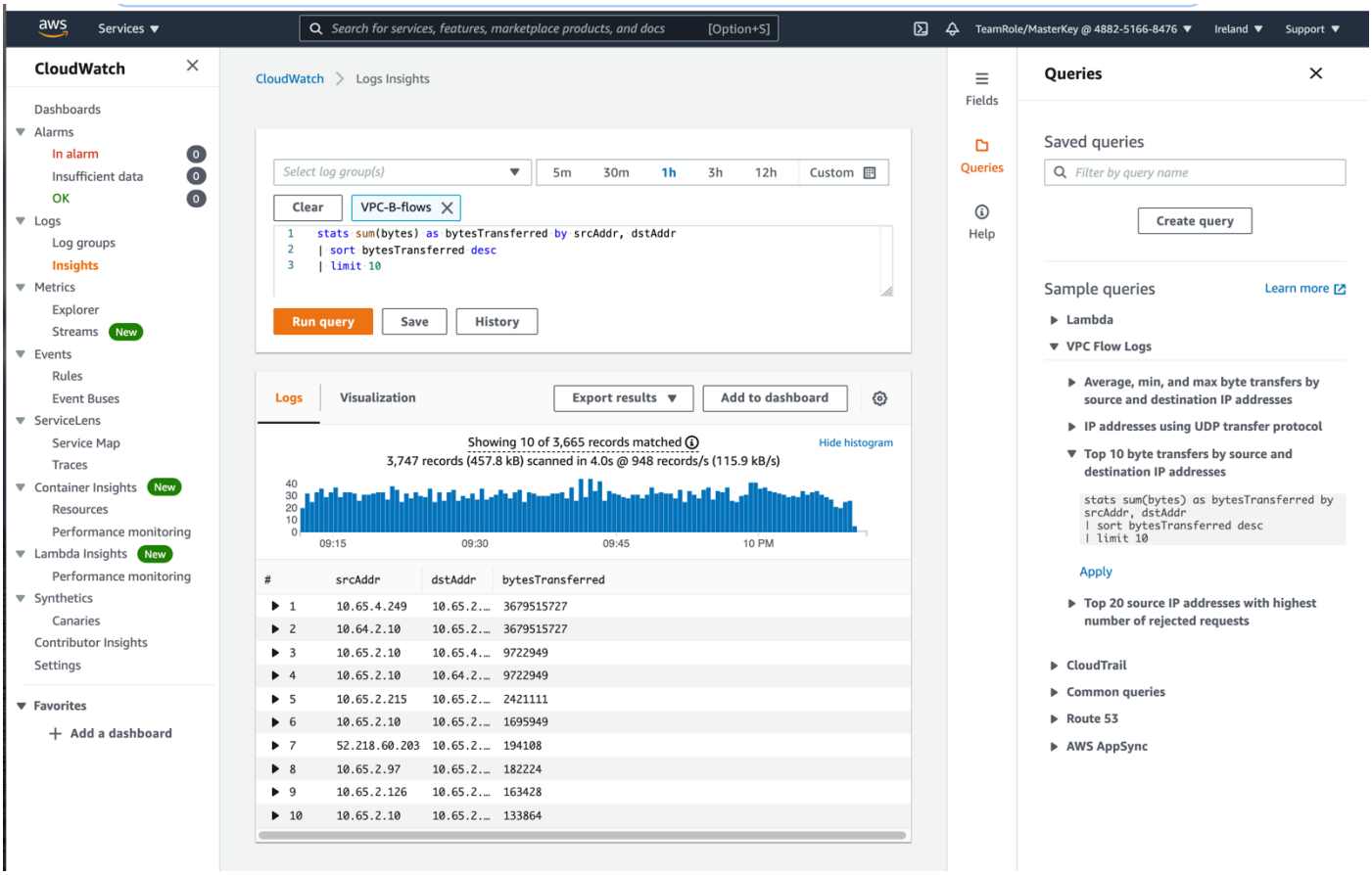
1.4 Sprawdź logi w CloudWatch

Wejdź do log grupy i przejrzyj informacje dostępne w serwisie CloudWatch.



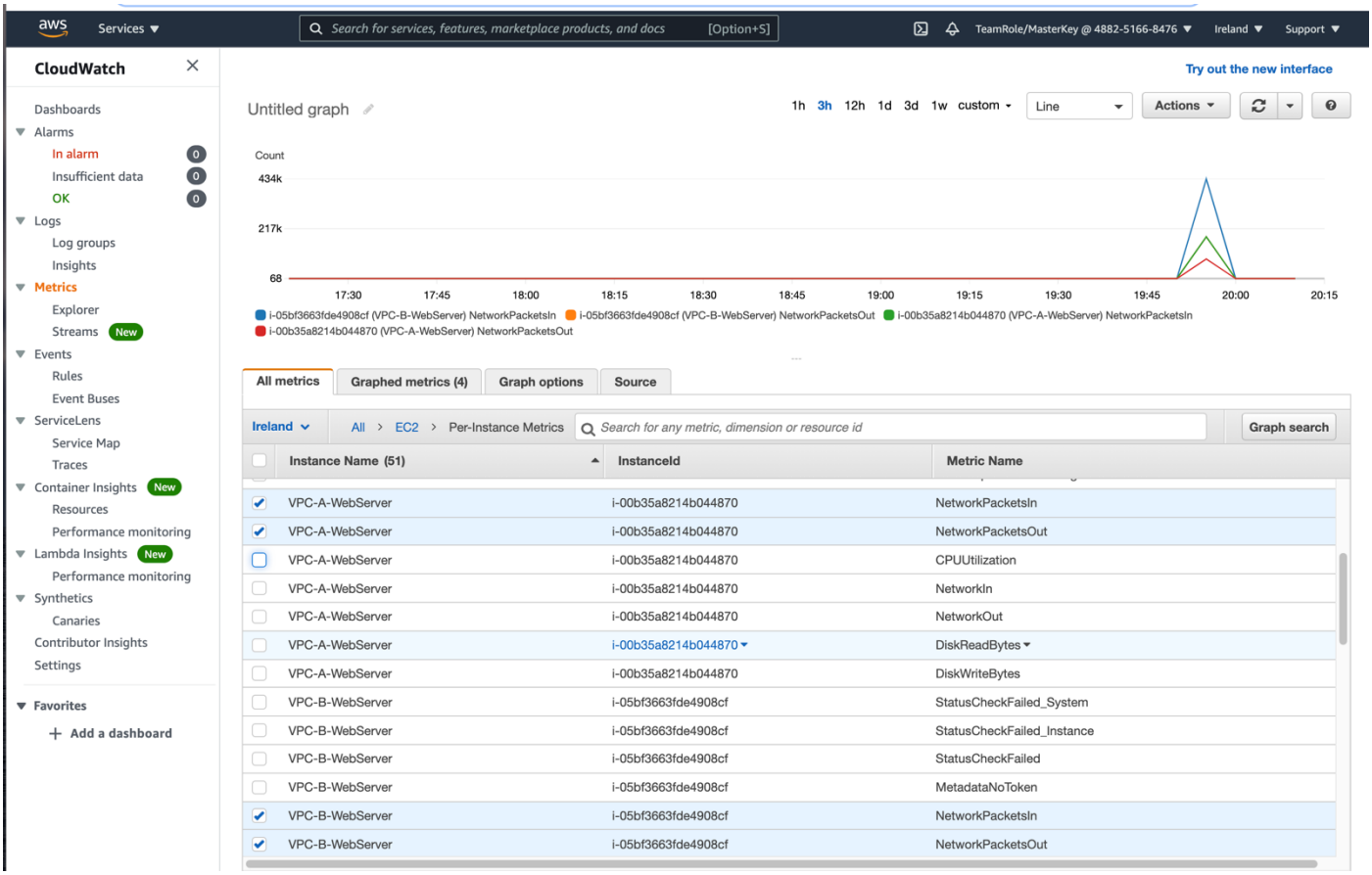
1.5 Poznaj możliwości przeszukiwania Logs Insights

Otwórz Log Insights i zapoznaj się z przykładowymi kwerendami pokazującymi możliwości filtrowania flow logów.



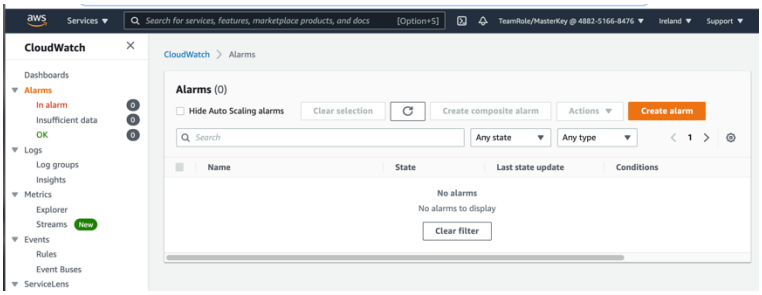
1.6 Poznaj dostępne metryki

Otwórz Metrics wybierając z lewego menu. Wybór metryk jest ograniczony do tych, które zostały zapisane i są dostępne do przeglądania w CloudWatch. Powinniśmy zaobserwować pakiety, które wysyłaliśmy z jednego serwera do drugiego.

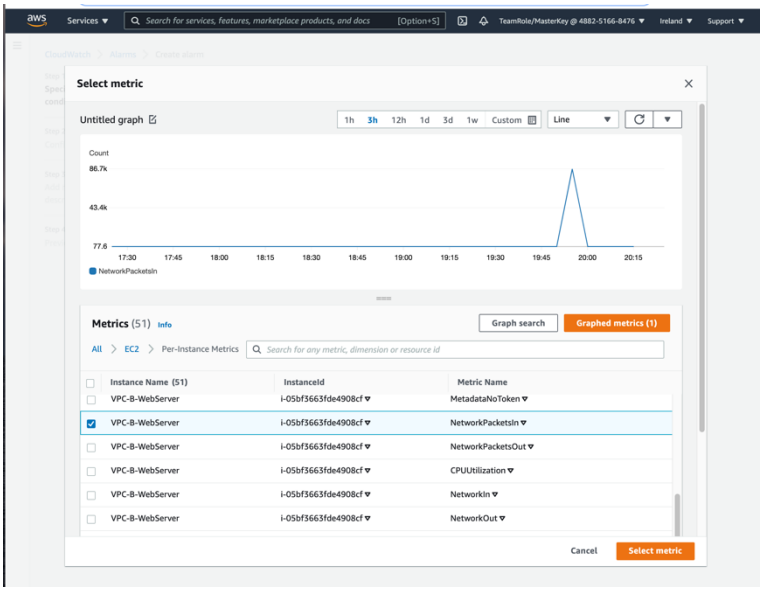


1.7 Zdefiniuj reakcję na sytuację wyjątkową

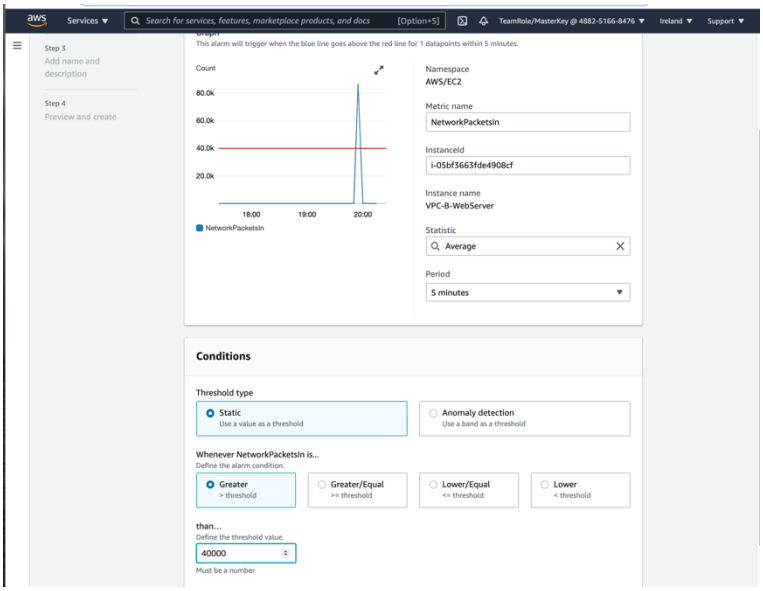
Wybierz z lewego menu **Alarms** i polecenie Create alarm.



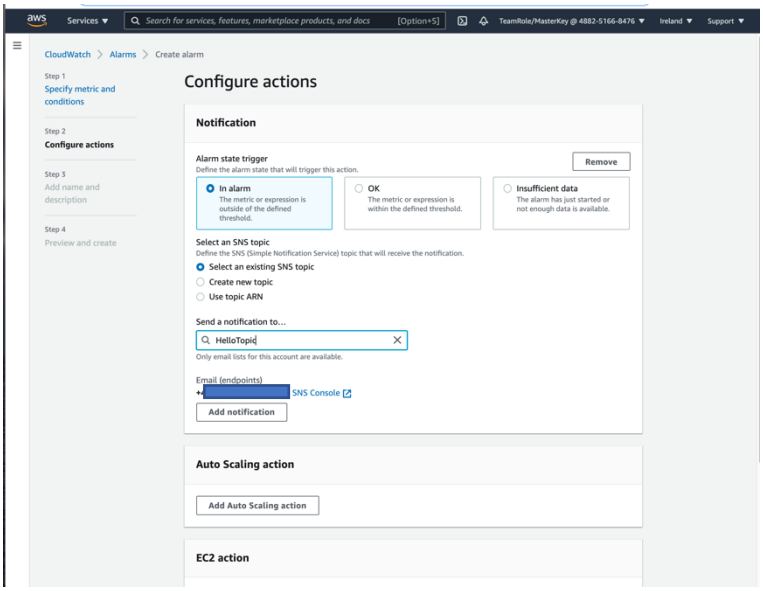
Wybierz metrykę dla serwera VPC-B-WebServer **NetworkPacketsIn**.



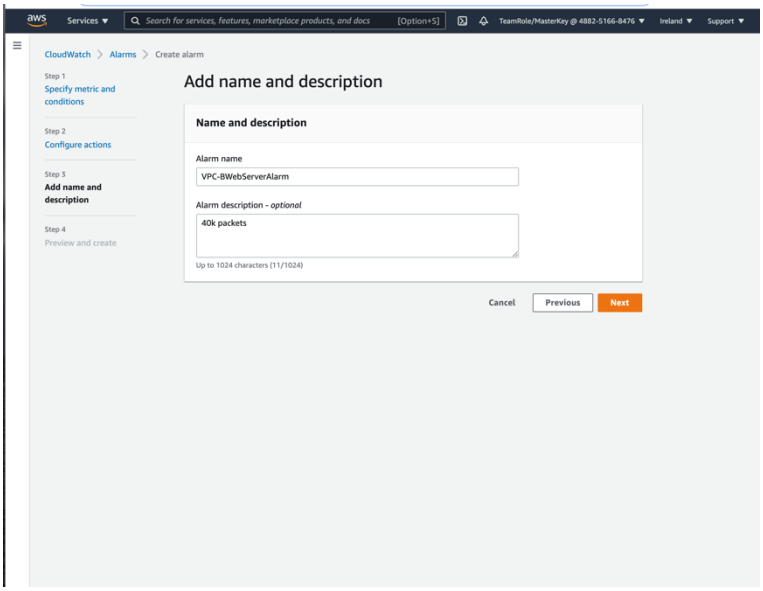
Określ warunki, kiedy alarm powinien się włączyć. Na przykład dla ilości pakietów powyżej 40k. Zmień również okres próbkowania do 1 minuty.



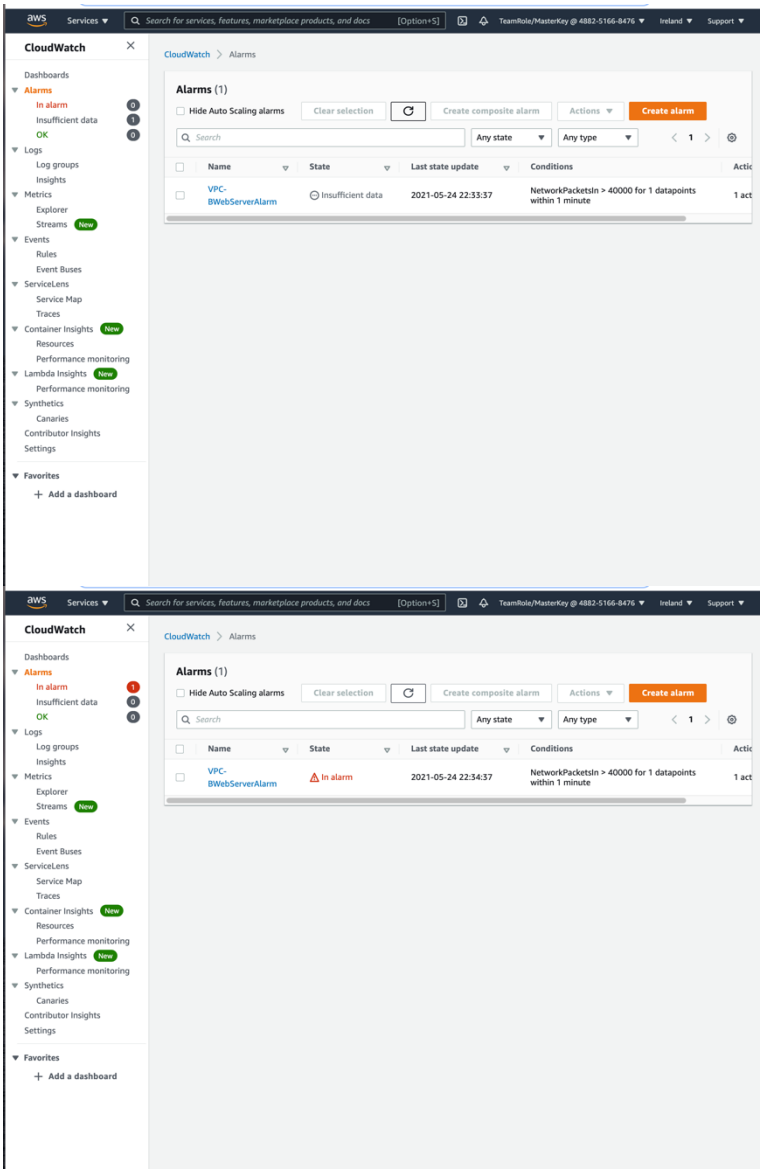
Ustaw powiadomienie w przypadku włączenia się alarmu. Wybierz wcześniej stworzony **HelloTopic**.



Nadaj nazwę dla alarmu.

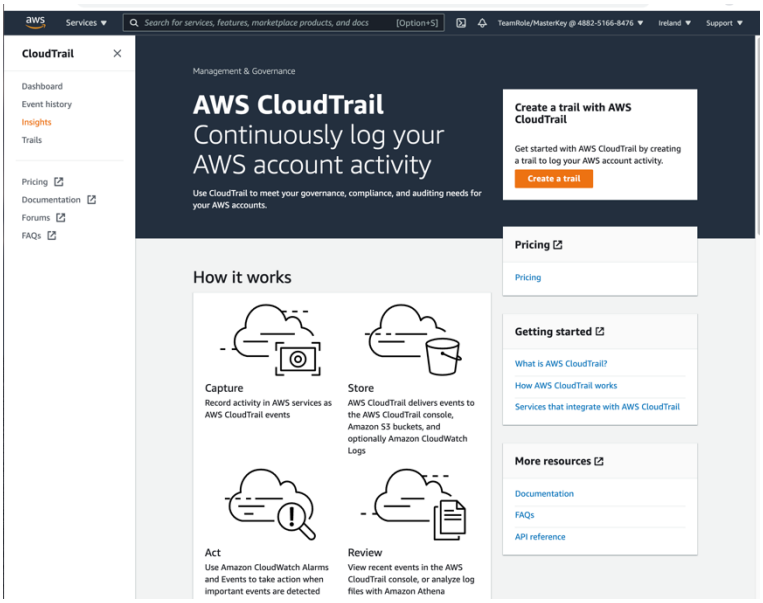


Teraz powtórnie uruchom transfer iperf3 z maszyny A do maszyny B i zaczekaj na powiadomienie. Po około 2 minutach, powinieneś dostać sms lub email w zależności od rodzaju subskrypcji jaką ustawiłeś w poprzednim ćwiczeniu.



1.8 Sprawdź co się działo z konfiguracją na koncie AWS

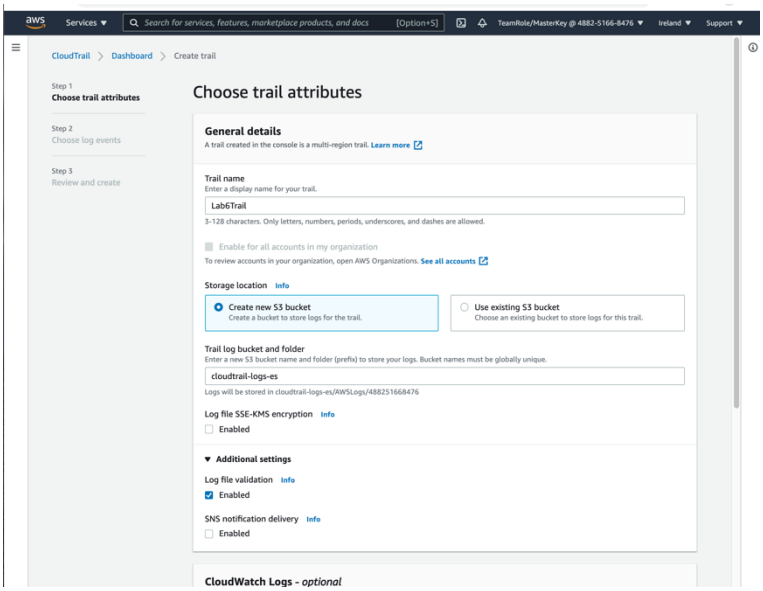
Wybierz usługę CloudTrail i wybierz Create Trail.



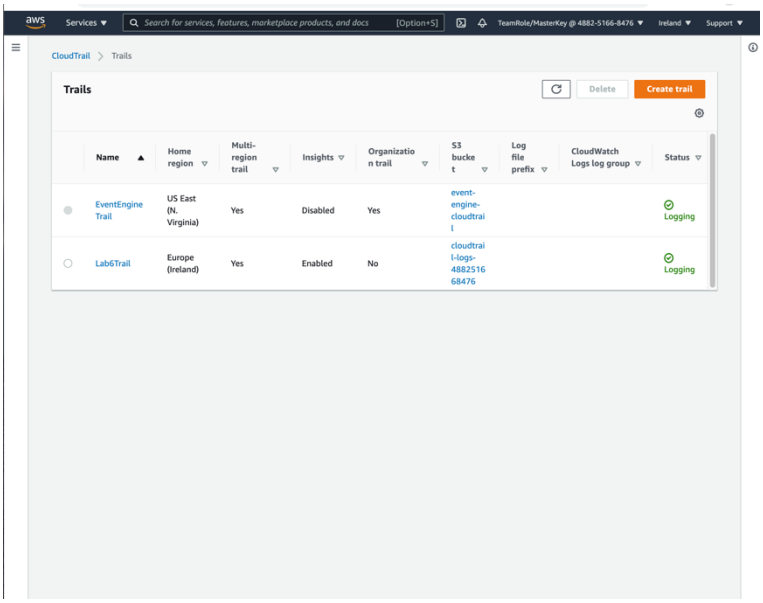
Podaj dane do konfiguracji:

- Nazwę konfiguracji
- Unikalną nazwę koszyka do zapisania informacji

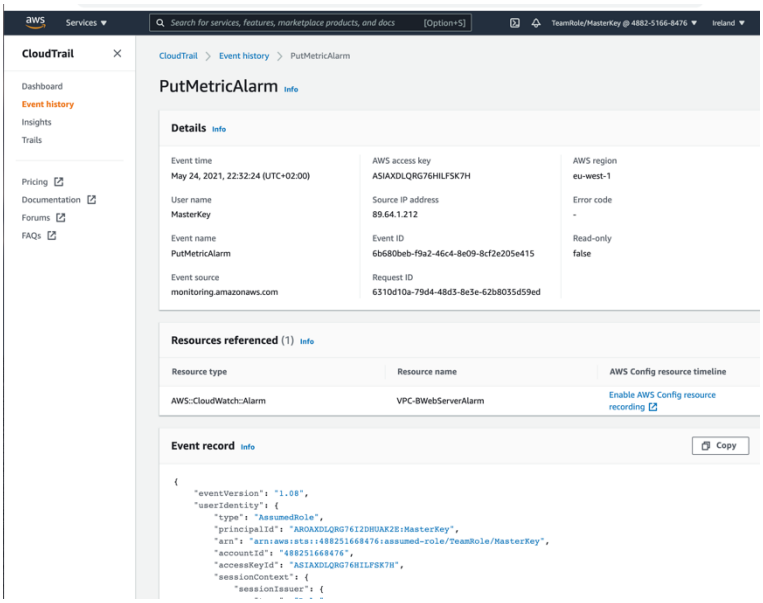
- Wyłącz enkrypcję
- Wybierz **Next**



Utwórz trail. Na koncie jest już włączone logowanie akcji w EventEngineTrail, tam znajdą się wszystkie twoje działania zalogowane.



Wybierz Event history i zobacz co jest widoczne dla ostatniej akcji, w której definiowałeś Alarm.



Ukończyłeś ćwiczenie!