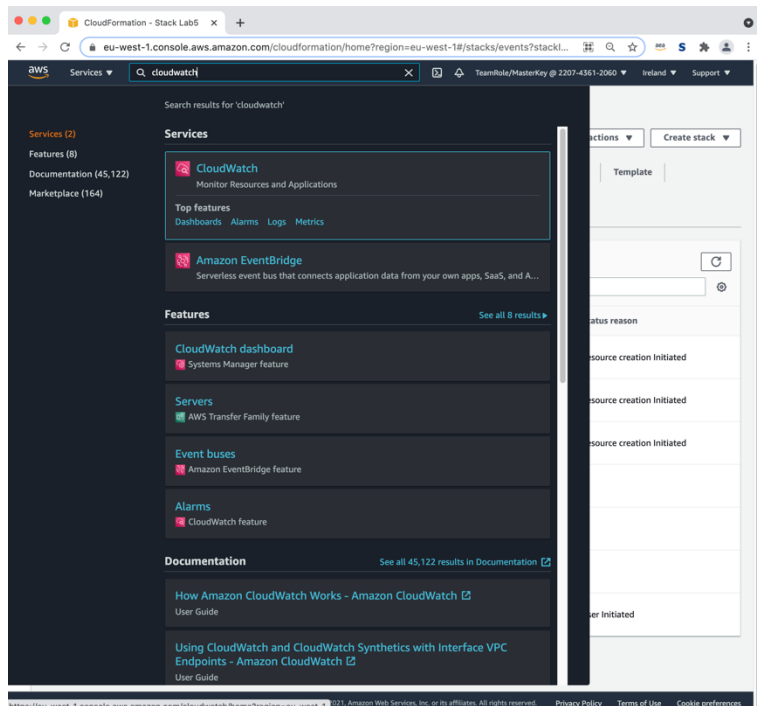


## ĆWICZENIE NR 6

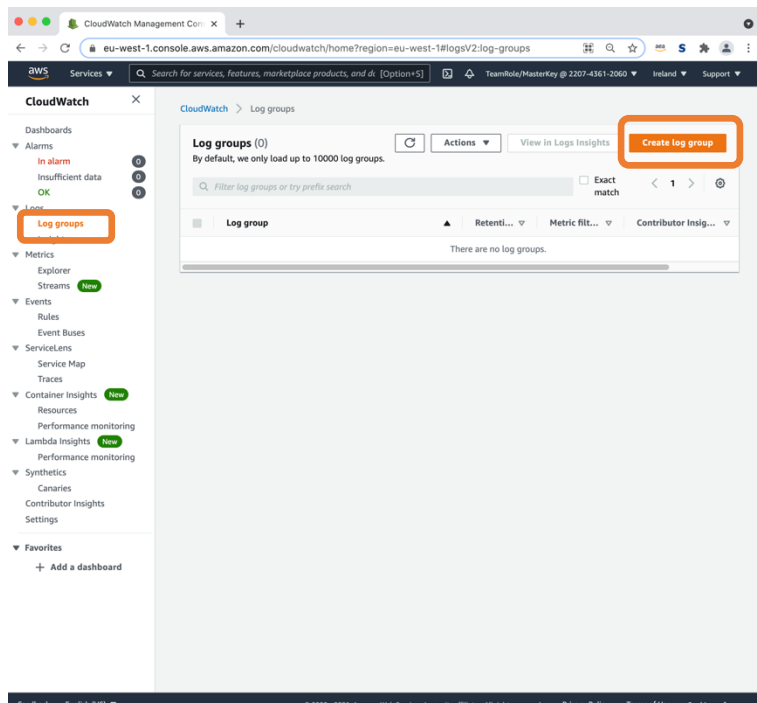
W tym ćwiczeniu korzystając z konfiguracji z ćwiczenia 5 podejrzmy co widać w logach.

### 1.1 Przygotuj log grupy dla VPC

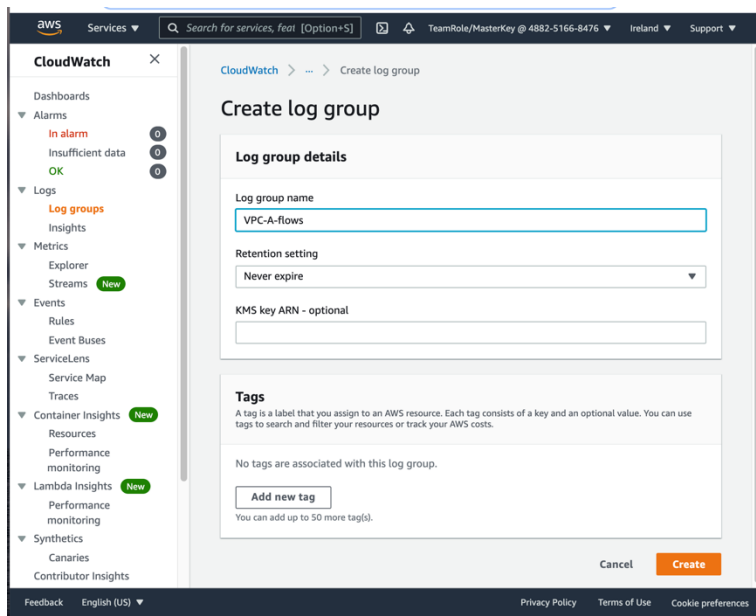
Wybierz stronę usługi CloudWatch.



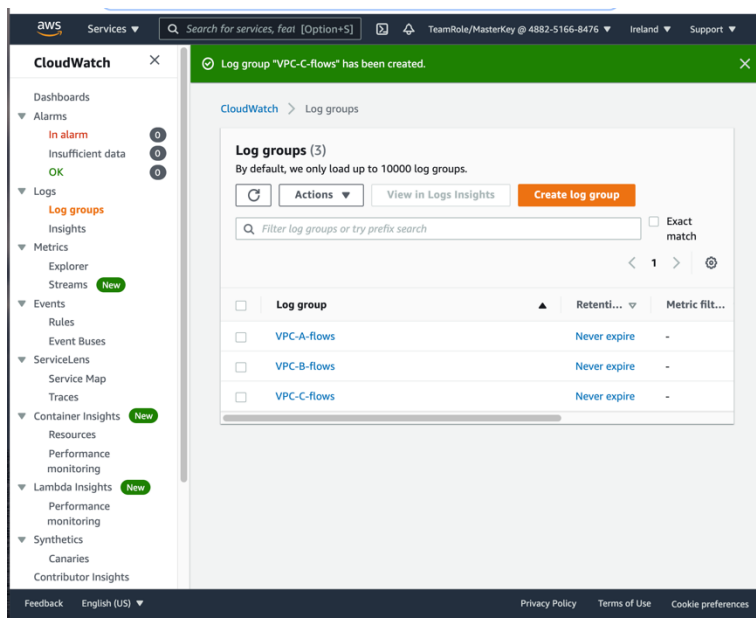
Z lewej strony z menu wybierz **Log groups**, a następnie **Create log group**.



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

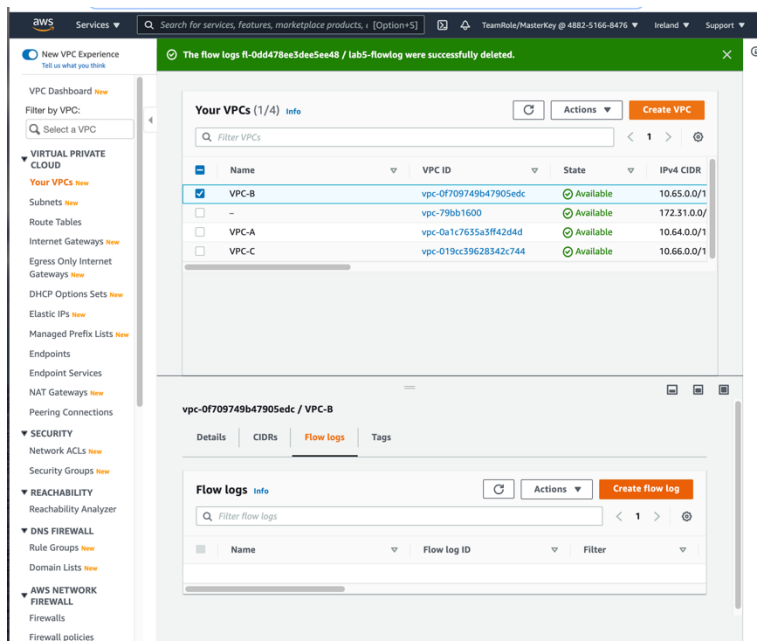


Do obserwacji różnych VPC rekomendowane jest definiowanie oddzielnych grup logujących (nie jest to wymagane).



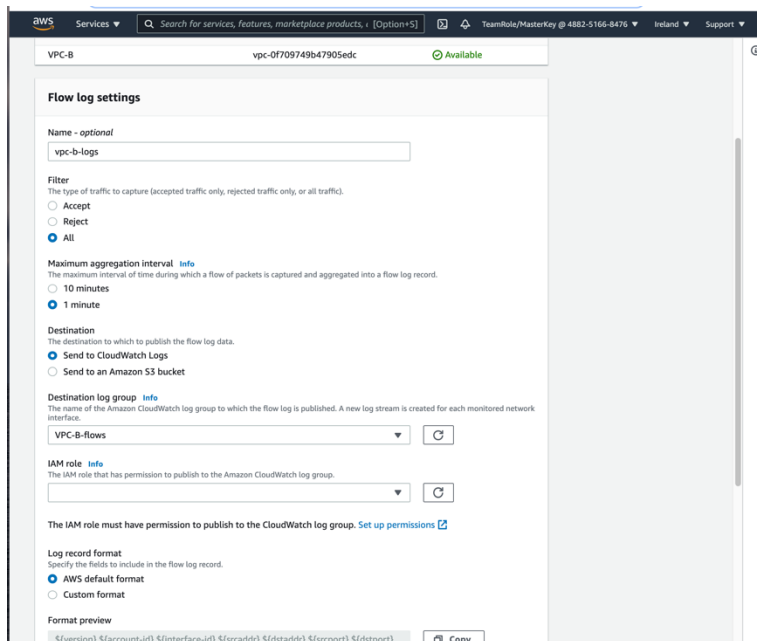
## 1.2 Włącz logowanie dla VPC

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

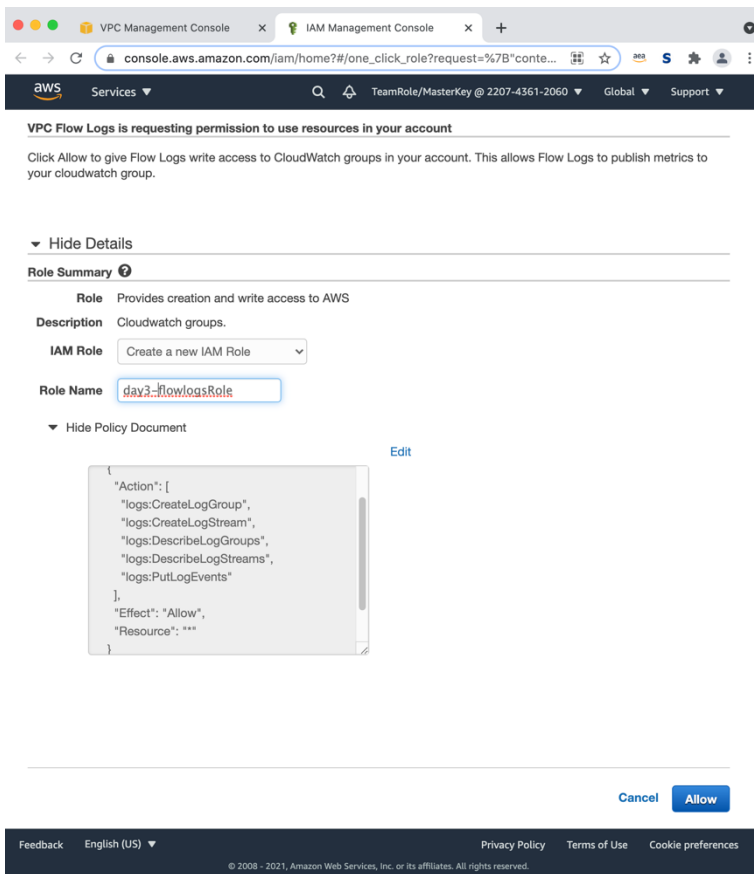


Podaj dane do konfiguracji logowania:

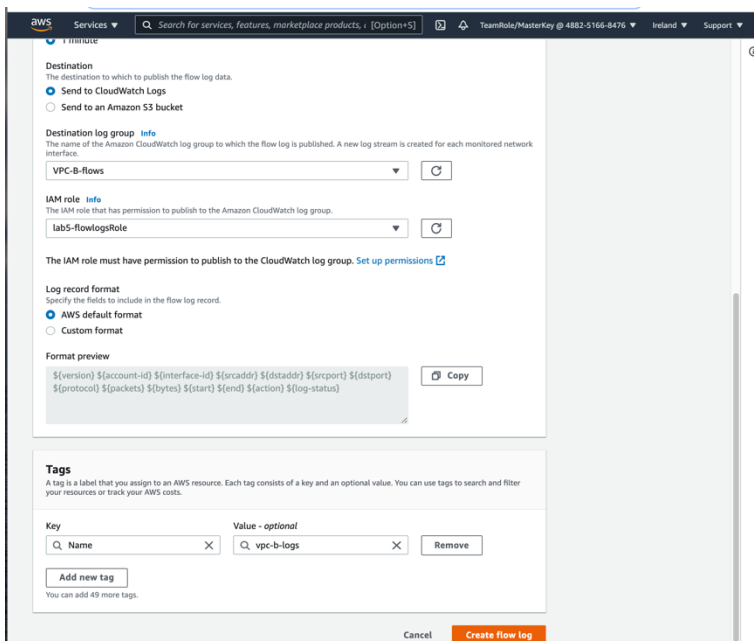
- Nazwa konfiguracji
- Filtrowanie – wybierz All
- Minimum aggregation interval – wybierz 1 minute
- Destination pozostaw CloudWatch i wybierz log grupę
- Otwórz link **Set up permissions**



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



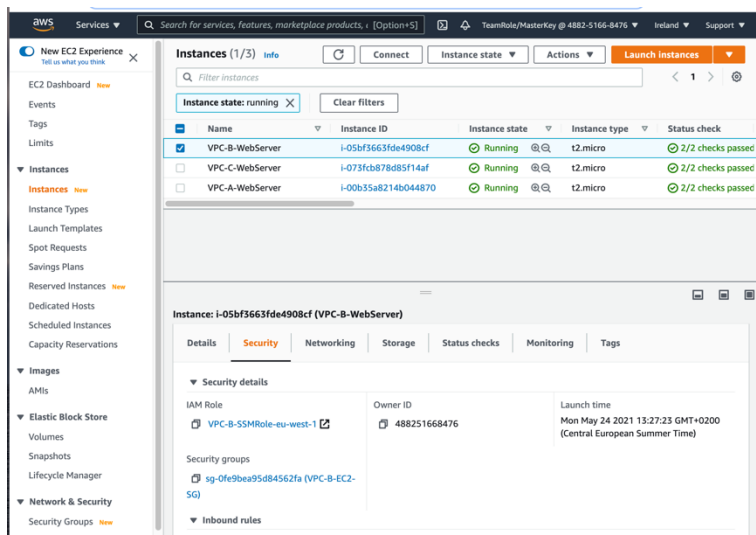
Odśwież wybór dla IAM role i wybierz rolę wcześniej przygotowaną w oddzielnej zakładce przeglądarki.



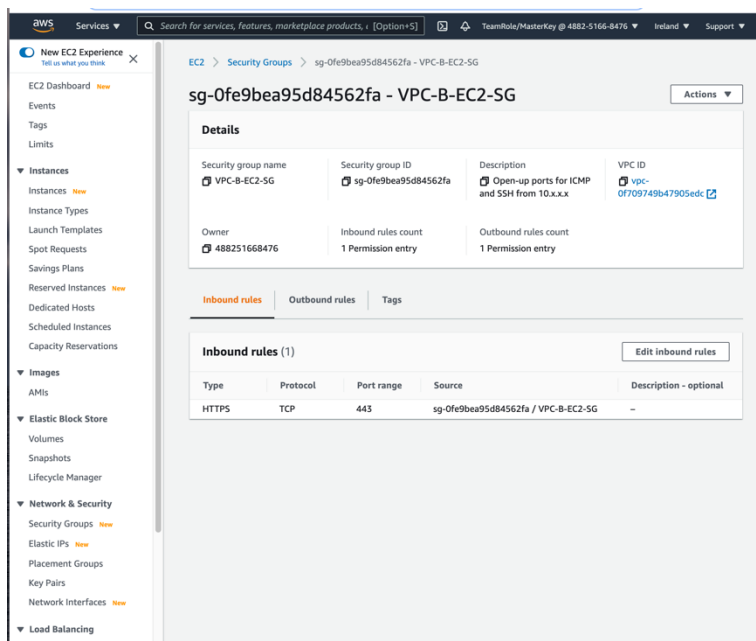
Zapisz konfigurację logowania. Możesz też ustawić logowanie w innych VPC.

### 1.3 Wygeneruj ruch sieciowy

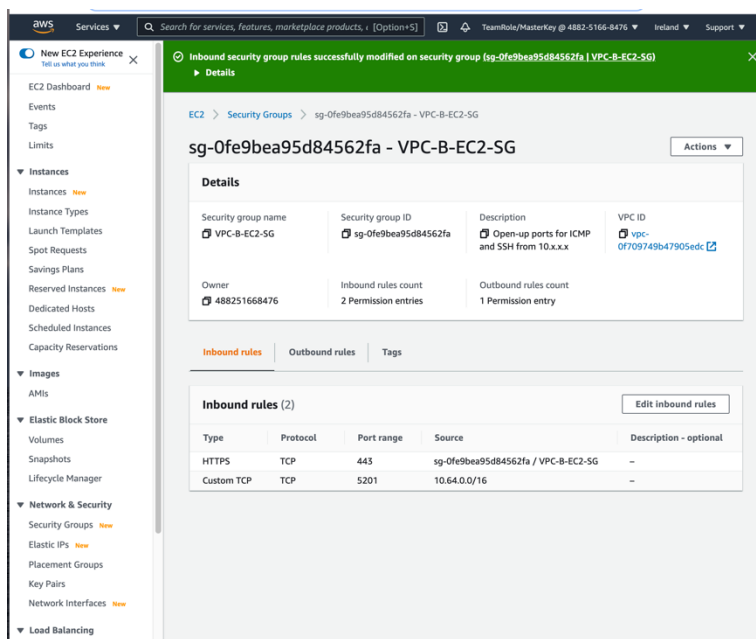
Wybierz serwer wirtualny z VPC-B oraz zakładkę **security** na stronie usługi EC2.



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
```

```
Session ID: MasterKey-Qa2e041530acfc77 Instance ID: i-05bf3663fde4908cf Terminate
sh-4.2$ sudo yum install iperf3 -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amazon2-core | 3.7 kB 00:00:00
amazon2-docker | 3.0 kB 00:00:00
Resolving Dependencies
--> Running transaction check
--> Package iperf3.x86_64 0:3.1.7-2.amzn2.0.2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
iperf3 x86_64 3.1.7-2.amzn2.0.2 amazon2-core 79 k

Transaction Summary
=====
Install 1 Package

Total download size: 79 k
Installed size: 196 k
Downloading packages:
iperf3-3.1.7-2.amzn2.0.2.x86_64.rpm | 79 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : iperf3-3.1.7-2.amzn2.0.2.x86_64 1/1
Verifying : iperf3-3.1.7-2.amzn2.0.2.x86_64 1/1

Installed:
iperf3.x86_64 0:3.1.7-2.amzn2.0.2

Complete!
sh-4.2$ iperf3 -s
Server listening on 5201
=====
```

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.

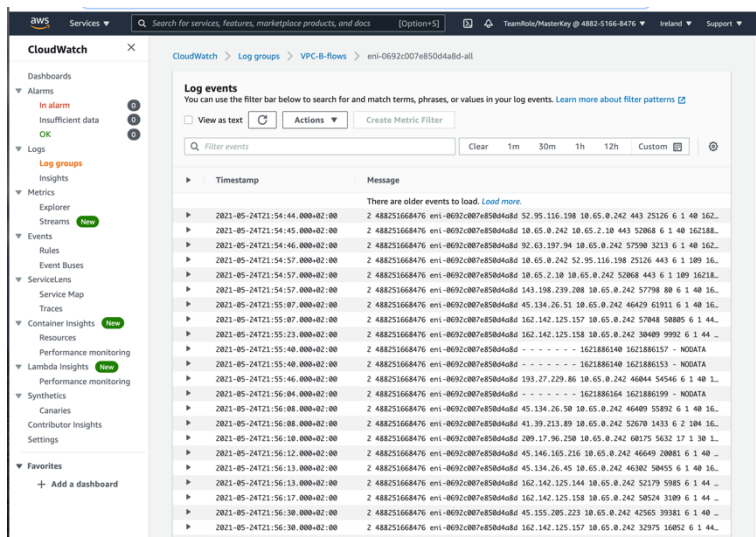
```
iperf3 -c 10.65.2.10 -P 2 -t 30
```

```
Session ID: MasterKey-0368d007262e7ba5a Instance ID: i-00b35a8214b044870
[ 15] 18.00-19.00 sec 28.4 MBytes 238 Mbits/sec 0 478 KBytes
[SUM] 18.00-19.00 sec 57.4 MBytes 483 Mbits/sec 0
-----
[ 4] 19.00-20.00 sec 30.7 MBytes 257 Mbits/sec 0 478 KBytes
[ 15] 19.00-20.00 sec 29.5 MBytes 247 Mbits/sec 0 487 KBytes
[SUM] 19.00-20.00 sec 60.2 MBytes 504 Mbits/sec 0
-----
[ 4] 20.00-21.00 sec 36.5 MBytes 306 Mbits/sec 0 536 KBytes
[ 15] 20.00-21.00 sec 39.4 MBytes 331 Mbits/sec 0 544 KBytes
[SUM] 20.00-21.00 sec 75.9 MBytes 637 Mbits/sec 0
-----
[ 4] 21.00-22.00 sec 110 MBytes 925 Mbits/sec 39 421 KBytes
[ 15] 21.00-22.00 sec 112 MBytes 941 Mbits/sec 43 404 KBytes
[SUM] 21.00-22.00 sec 222 MBytes 1.87 Gbits/sec 82
-----
[ 4] 22.00-23.00 sec 59.5 MBytes 499 Mbits/sec 23 503 KBytes
[ 15] 22.00-23.00 sec 57.9 MBytes 486 Mbits/sec 29 239 KBytes
[SUM] 22.00-23.00 sec 117 MBytes 985 Mbits/sec 52
-----
[ 4] 23.00-24.00 sec 72.2 MBytes 606 Mbits/sec 8 396 KBytes
[ 15] 23.00-24.00 sec 46.5 MBytes 390 Mbits/sec 7 371 KBytes
[SUM] 23.00-24.00 sec 119 MBytes 995 Mbits/sec 15
-----
[ 4] 24.00-25.00 sec 70.6 MBytes 592 Mbits/sec 8 322 KBytes
[ 15] 24.00-25.00 sec 48.8 MBytes 409 Mbits/sec 14 412 KBytes
[SUM] 24.00-25.00 sec 119 MBytes 1.00 Gbits/sec 22
-----
[ 4] 25.00-26.00 sec 58.4 MBytes 490 Mbits/sec 11 363 KBytes
[ 15] 25.00-26.00 sec 59.8 MBytes 502 Mbits/sec 11 322 KBytes
[SUM] 25.00-26.00 sec 118 MBytes 992 Mbits/sec 22
-----
[ 4] 26.00-27.00 sec 56.8 MBytes 477 Mbits/sec 12 495 KBytes
[ 15] 26.00-27.00 sec 62.1 MBytes 521 Mbits/sec 14 206 KBytes
[SUM] 26.00-27.00 sec 119 MBytes 998 Mbits/sec 26
-----
[ 4] 27.00-28.00 sec 60.3 MBytes 506 Mbits/sec 12 322 KBytes
[ 15] 27.00-28.00 sec 57.1 MBytes 479 Mbits/sec 8 363 KBytes
[SUM] 27.00-28.00 sec 117 MBytes 985 Mbits/sec 20
-----
[ 4] 28.00-29.00 sec 70.9 MBytes 595 Mbits/sec 12 412 KBytes
[ 15] 28.00-29.00 sec 48.7 MBytes 409 Mbits/sec 11 289 KBytes
[SUM] 28.00-29.00 sec 120 MBytes 1.00 Gbits/sec 23
-----
[ 4] 29.00-30.00 sec 66.5 MBytes 558 Mbits/sec 7 437 KBytes
[ 15] 29.00-30.00 sec 51.3 MBytes 430 Mbits/sec 11 297 KBytes
[SUM] 29.00-30.00 sec 118 MBytes 988 Mbits/sec 18
-----
[ ID] Interval Transfer Bandwidth Retr
[ 4] 0.00-30.00 sec 1.81 GBytes 519 Mbits/sec 394 sender
[ 4] 0.00-30.00 sec 1.81 GBytes 518 Mbits/sec 0 receiver
[ 15] 0.00-30.00 sec 1.60 GBytes 458 Mbits/sec 430 sender
[ 15] 0.00-30.00 sec 1.60 GBytes 457 Mbits/sec 0 receiver
[SUM] 0.00-30.00 sec 3.41 GBytes 977 Mbits/sec 824 sender
[SUM] 0.00-30.00 sec 3.41 GBytes 975 Mbits/sec 0 receiver

iperf Done.
sh-4.2$
```

## 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.

**CloudWatch > Logs Insights**

Select log group(s): **VPC-B-flows**

Clear **VPC-B-flows**

```
1 stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
2 | sort bytesTransferred desc
3 | limit 10
```

Run query Save History

**Logs Visualization** Export results Add to dashboard

Showing 10 of 3,665 records matched  
3,747 records (457.8 kB) scanned in 4.0s @ 948 records/s (115.9 kB/s)

#	srcAddr	dstAddr	bytesTransferred
1	10.65.4.249	10.65.2...	3679515727
2	10.64.2.10	10.65.2...	3679515727
3	10.65.2.10	10.65.4...	9722949
4	10.65.2.10	10.64.2...	9722949
5	10.65.2.215	10.65.2...	2421111
6	10.65.2.10	10.65.2...	1695949
7	52.218.60.203	10.65.2...	194108
8	10.65.2.97	10.65.2...	182224
9	10.65.2.126	10.65.2...	163428
10	10.65.2.10	10.65.2...	133864

**Queries**

Saved queries

Filter by query name

Create query

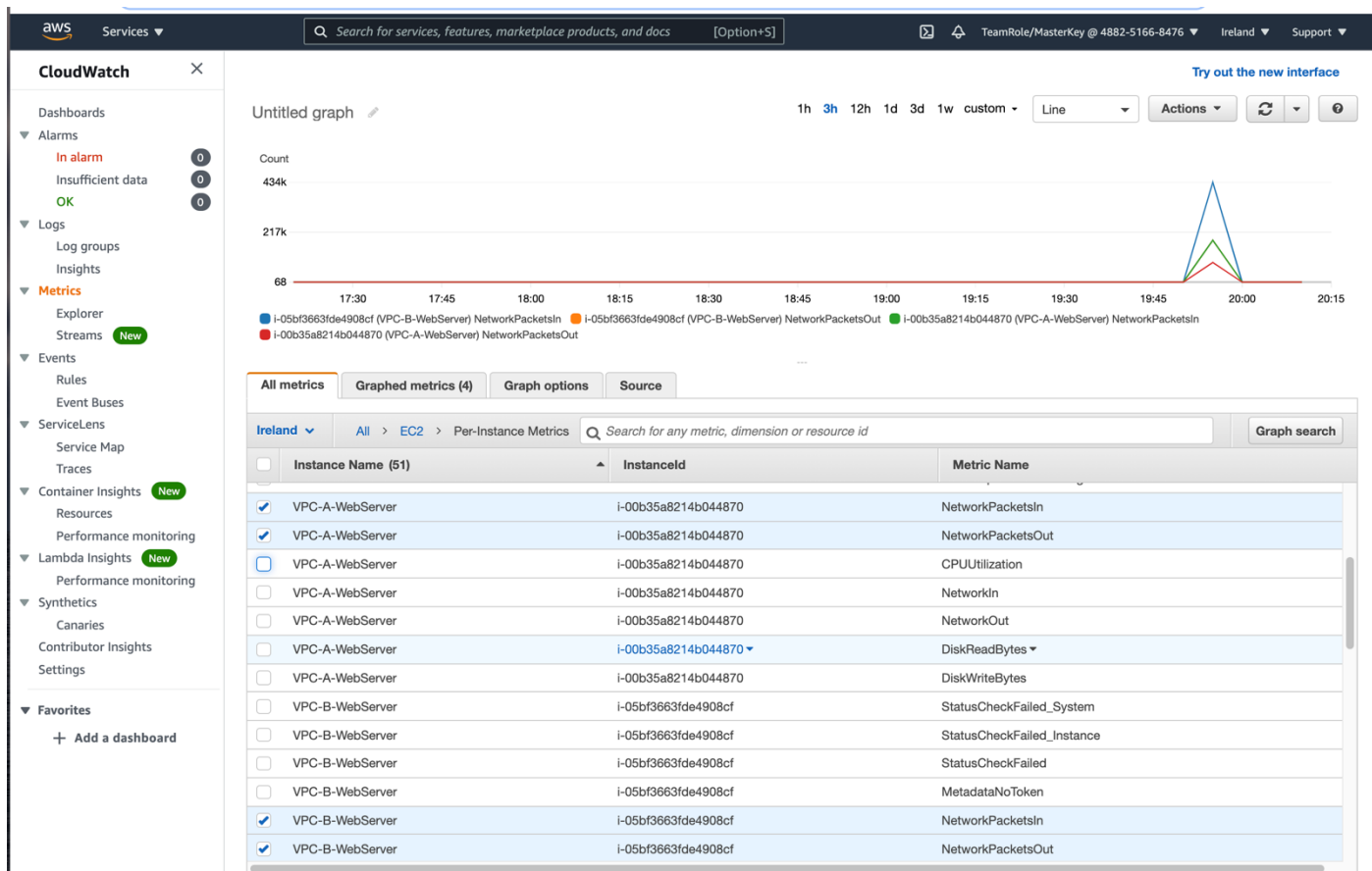
Sample queries [Learn more](#)

- Lambda
- VPC Flow Logs
  - Average, min, and max byte transfers by source and destination IP addresses
  - IP addresses using UDP transfer protocol
  - Top 10 byte transfers by source and destination IP addresses
 

```
stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
| sort bytesTransferred desc
| limit 10
```
- CloudTrail
- Common queries
- Route 53
- AWS AppSync

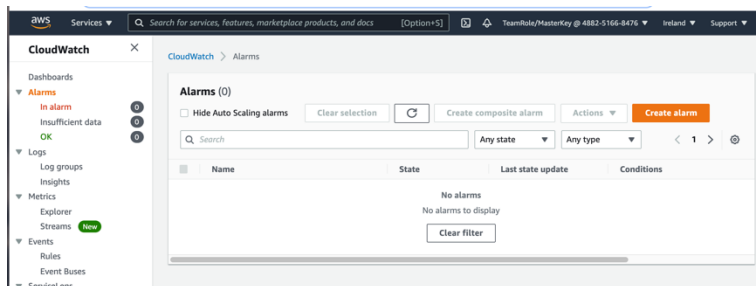
## 1.6 Poznaj dostępne metryki

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 wysyłałyśmy z jednego serwera do drugiego.

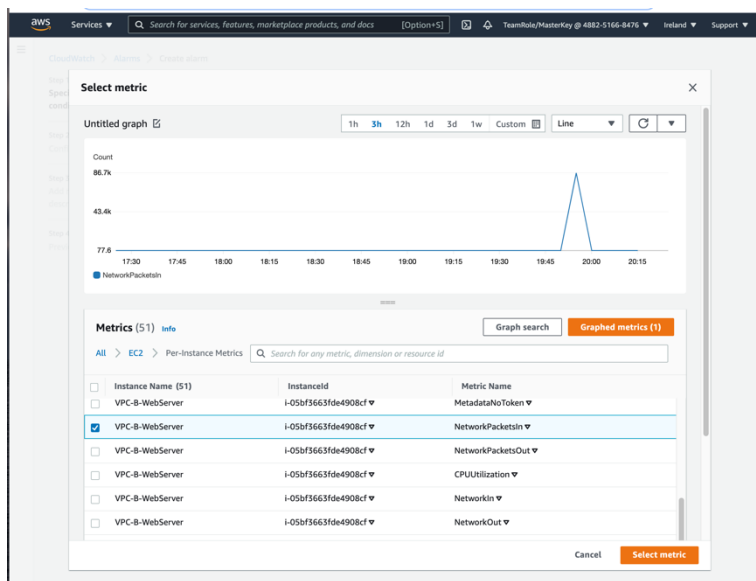


## 1.7 Zdefiniuj reakcję na sytuację wyjątkową

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.



This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Count

80.0k

60.0k

40.0k

20.0k

18:00 19:00 20:00

NetworkPacketsIn

Namespace  
AWS/EC2

Metric name  
NetworkPacketsIn

InstanceId  
i-05bf3663fde4908cf

Instance name  
VPC-B-WebServer

Statistic  
Average

Period  
5 minutes

**Conditions**

Threshold type

☒ Static  
Use a value as a threshold

☐ Anomaly detection  
Use a band as a threshold

Whenever NetworkPacketsIn is...

Define the alarm condition.

☒ Greater  
> threshold

☐ Greater/Equal  
>= threshold

☐ Lower/Equal  
<= threshold

☐ Lower  
< threshold

than...

Define the threshold value.

40000

Must be a number

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

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

**Configure actions**

**Notification**

Alarm state trigger  
Define the alarm state that will trigger this action.

☒ In alarm  
The metric or expression is outside of the defined threshold.

☐ OK  
The metric or expression is within the defined threshold.

☐ Insufficient data  
The alarm has just started or not enough data is available.

Select an SNS topic  
Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ Select an existing SNS topic

☐ Create new topic

☐ Use topic ARN

Send a notification to...

HelloTopic

Only email lists for this account are available.

Email (endpoints)

SNS Console

Add notification

**Auto Scaling action**

Add Auto Scaling action

**EC2 action**

Nadaj nazwę dla alarmu.

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

**Add name and description**

Name and description

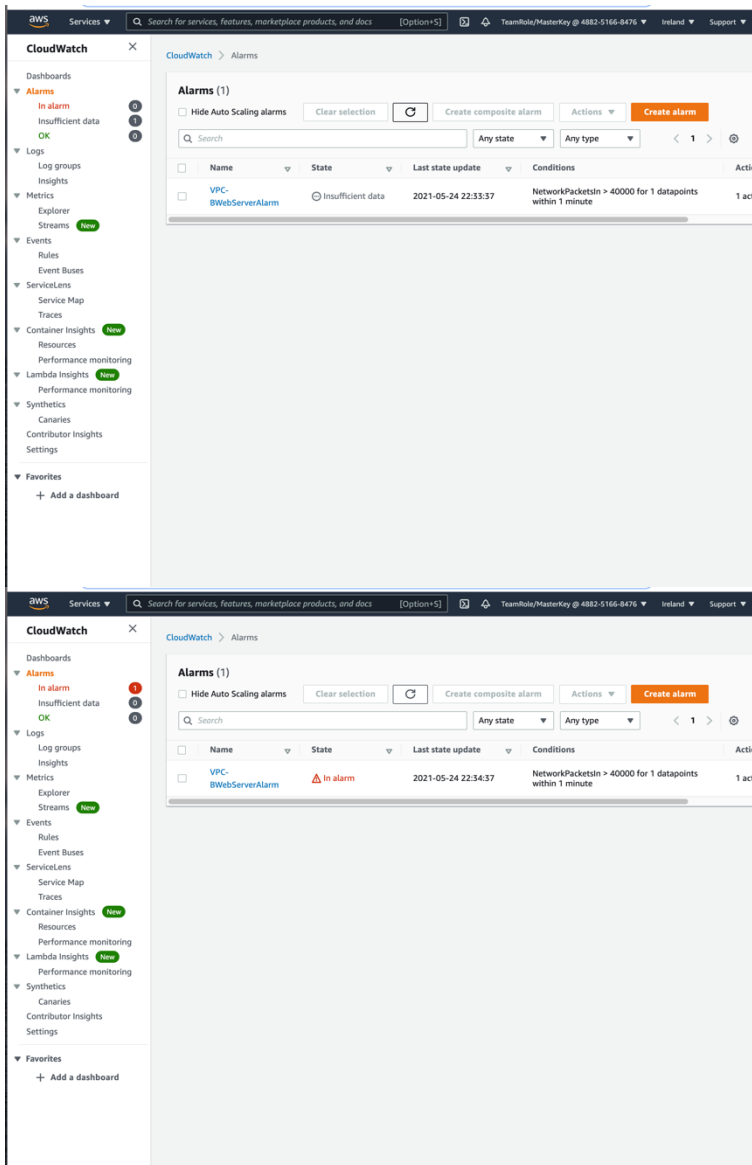
Alarm name  
VPC-B-WebServerAlarm

Alarm description - optional  
40k packets

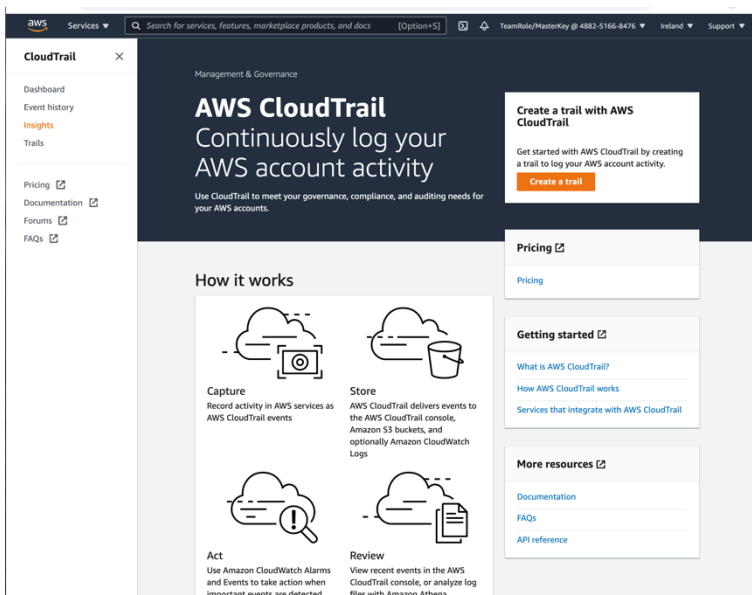
Up to 1024 characters (11/1024)

Cancel Previous Next

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**

Services ▾

Search for services, features, marketplace products, and docs [Option+5]

Team/Role/Masterkey @ 4882 5166-8476 ▾

inland ▾

Support ▾

CloudTrail ▾ Dashboard ▾ Create trail

Step 1  
Choose trail attributes

Step 2  
Choose log events

Step 3  
Review and create

## Choose trail attributes

### General details

A trail created in the console is a multi-region trail. [Learn more](#) ⓘ

**Trail name**  
Enter a display name for your trail.

Lab6Trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization  
To review accounts in your organization, open [AWS Organizations](#). [See all accounts](#) ⓘ

**Storage location** ⓘ

☒ Create new S3 bucket  
Create a new bucket to store logs for the trail.

☐ Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

**Trail log bucket and folder**  
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

cloudtrail-logs-es

Logs will be stored in cloudtrail-logs-es/RWSLogs/488251668476

**Log file SSE-KMS encryption** ⓘ

☐ Enabled

▼ **Additional settings**

**Log file validation** ⓘ

☒ Enabled

**SNS notification delivery** ⓘ

☐ Enabled

CloudWatch Logs - optional

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

aws

Services ▾

Search for services, features, marketplace products, and docs

[Option1-5]

TeamRole/MasterKey @ 4882-5166-8476 ▾

Ireland ▾

Support ▾

Trails

Trails

Delete

Create trail

	Name ▲	Home region ▾	Multi-region trail ▾	Insights ▾	Organization trail ▾	S3 bucket ▾	Log file prefix ▾	CloudWatch Logs log group ▾	Status ▾
●	EventEngine Trail	US East (N. Virginia)	Yes	Disabled	Yes	event-engine-cloudtrail			Logging
○	Lab6Trail	Europe (Ireland)	Yes	Enabled	No	cloudtrail-logs-488251668476			Logging

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

Services ▼
Search for services, features, marketplace products, and docs [Option+S]
 TeamRole/MasterKey @ 4882-5166-6476 Inland ▼

## CloudTrail

- Dashboard
- Event history**
- Insights
- Trails
  
- Pricing
- Documentation
- Forums
- FAQs

CloudTrail > Event history > PutMetricAlarm

# PutMetricAlarm Info

---

### Details Info

Event time	AWS access key	AWS region
May 24, 2021, 22:32:24 (UTC+02:00)	ASIAIDLQRG76HLPFK7H	eu-west-1
User name	Source IP address	Error code
MasterKey	89.64.1.212	-
Event name	Event ID	Read-only
PutMetricAlarm	6b680beb-f9a2-46c4-8e09-8cf2e205e415	false
Event source	Request ID	
monitoring.amazonaws.com	6310d10a-7944-48d5-8e3e-62b8035d59ed	

---

### Resources referenced Info

Resource type	Resource name	AWS Config resource timeline
AWS::CloudWatch::Alarm	VPC-BWebServerAlarm	<a href="#">Enable AWS Config resource recording </a>

---

### Event record Info

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAXDQLRG76I2DHUAKZE:MasterKey",
    "arn": "arn:aws:iam::488251668476:assumed-role/TeamRole/MasterKey",
    "accountId": "488251668476",
    "accessKeyId": "ASIAIDLQRG76HLPFK7H",
    "sessionContext": {
      "sessionIssuer": {
        "type": "AssumedRole",
        "principalId": "AROAXDQLRG76I2DHUAKZE:MasterKey",
        "arn": "arn:aws:iam::488251668476:assumed-role/TeamRole/MasterKey",
        "accountId": "488251668476",
        "accessKeyId": "ASIAIDLQRG76HLPFK7H",
        "sessionContext": {}
      }
    }
  },
  "sourceIp": "89.64.1.212",
  "eventName": "PutMetricAlarm",
  "eventType": "AwsApiCall",
  "eventCategory": "Management",
  "resources": [
    {
      "resourceType": "AWS::CloudWatch::Alarm",
      "resourceName": "VPC-BWebServerAlarm",
      "physicalResourceId": null,
      "logicalResourceId": "VPC-BWebServerAlarm"
    }
  ],
  "requestParameters": {
    "alarmConfiguration": {
      "name": "VPC-BWebServerAlarm",
      "stateValue": "OK",
      "actionsEnabled": true,
      "okActions": [
        "sns:Publish"
      ],
      "insufficientDataActions": [],
      "alarmActions": []
    }
  },
  "responseElements": {
    "CreateAlarmResponse": {
      "alarmArn": "arn:aws:cloudwatch:eu-west-1:488251668476:alarm:VPC-BWebServerAlarm",
      "alarmName": "VPC-BWebServerAlarm",
      "metricName": "CPUUsage",
      "namespace": "AWS/ECS",
      "period": 300,
      "statistic": "Average",
      "unit": "Percent",
      "evaluationPeriods": 1,
      "threshold": 80,
      "comparisonOperator": "GreaterThanOrEqualToThreshold",
      "treatMissingData": "FillByPreviousValue"
    }
  },
  "result": true,
  "errorCode": null,
  "errorMessage": null,
  "details": {}
}
```

Copy

Ukończyłeś ćwiczenie!