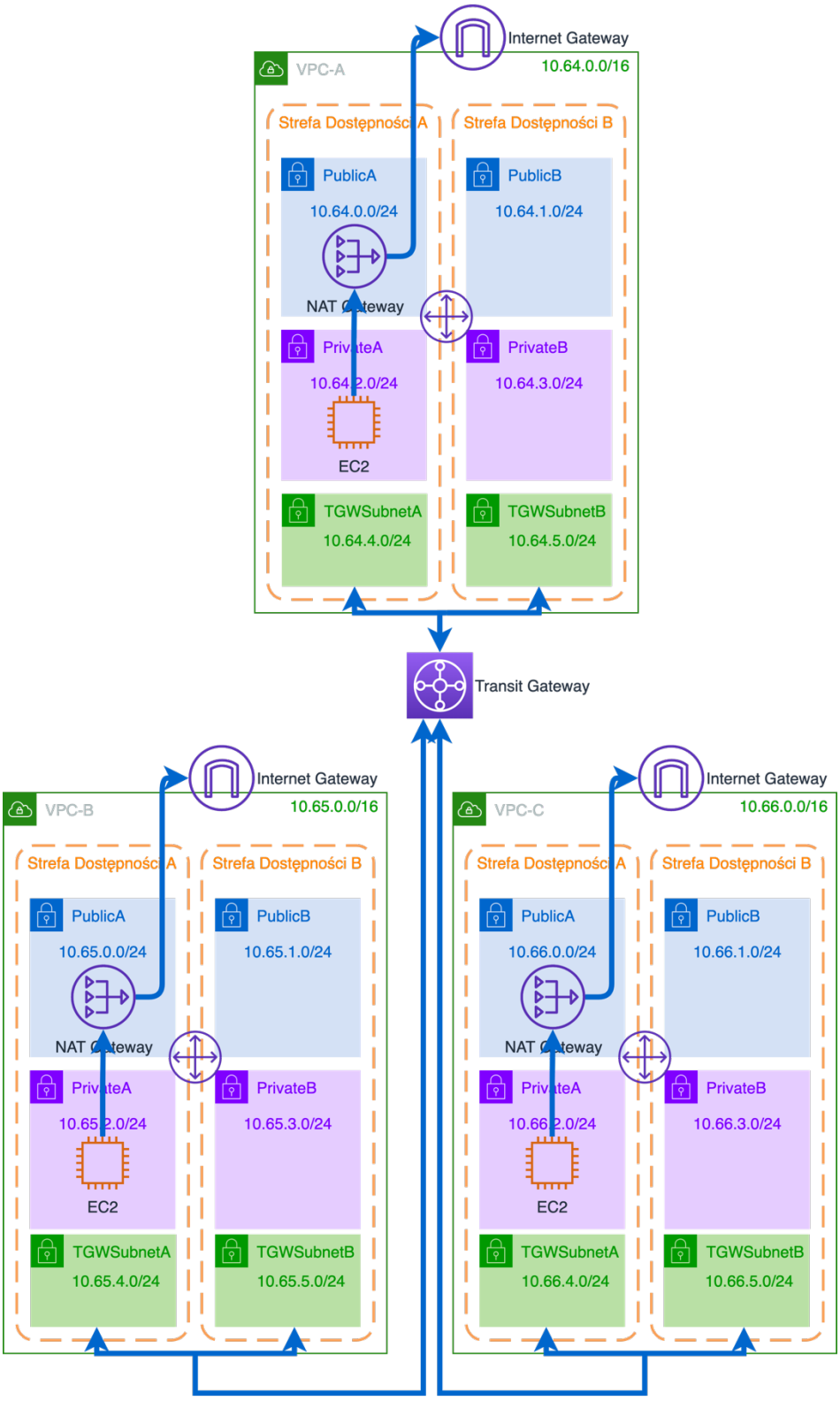
ĆWICZENIE NR 5

W tym ćwiczeniu połączymy się prywatnym interfejsem z usługą S3.

1.1 Przygotuj konfigurację startową

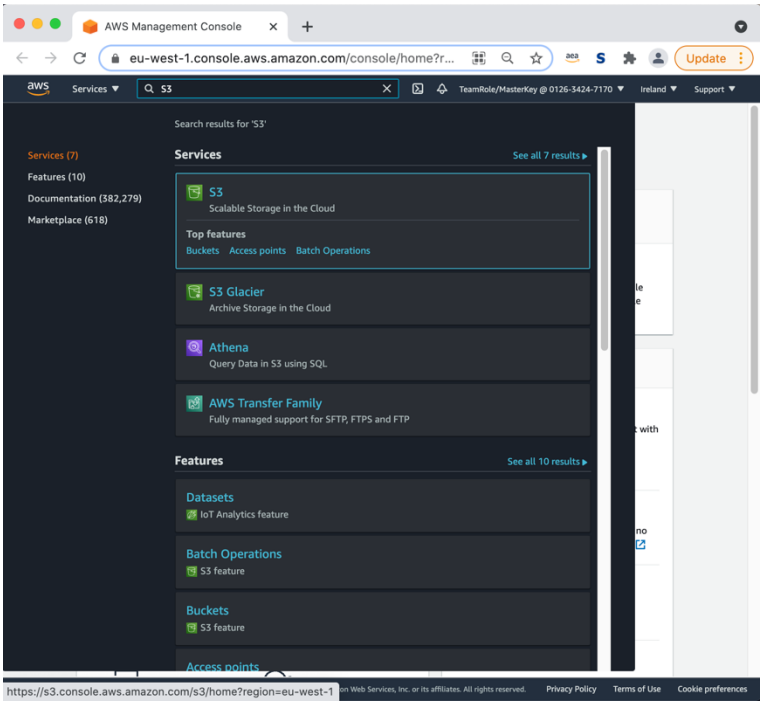
W ćwiczeniu 5 i 6 wykorzystamy konfigurację, jak w ćwiczeniu numer 2, trzech VPC połączonych przez TransitGateway. Konfiguracja pokazana jest na diagramie:



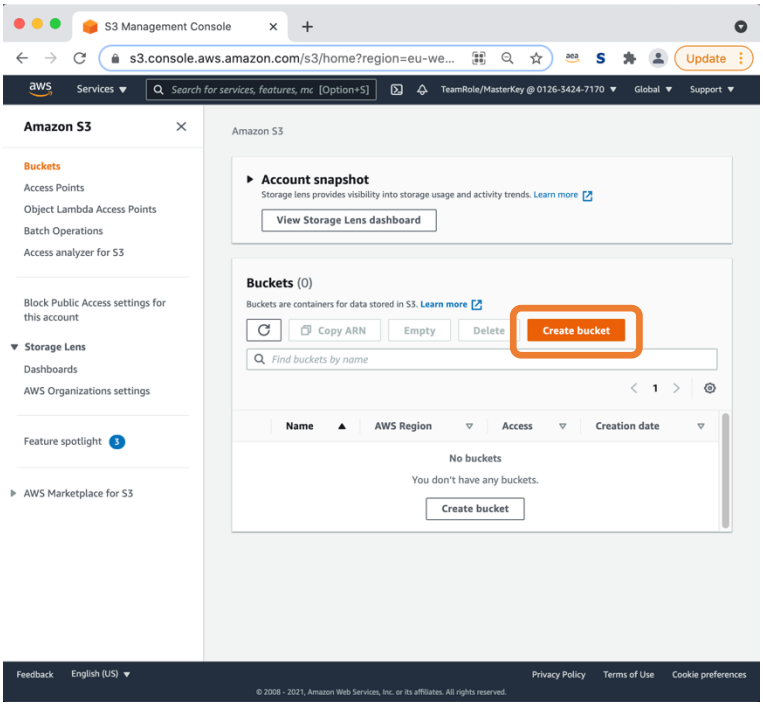
1.2 Wgraj skrypty konfiguracyjne na S3

Całość konfiguracji powołamy ze skryptu CloudFormation, żeby wykorzystać zagnieżdżone konfiguracje udostępnimy serwisowi CloudFormation skrypty do pobierania w S3.

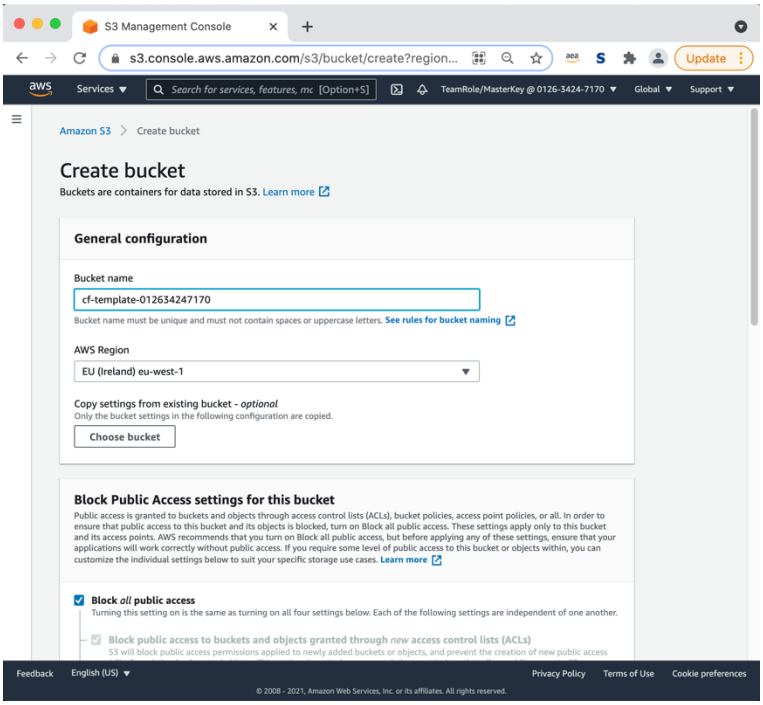
Wybierz z konsoli AWS usługę S3.



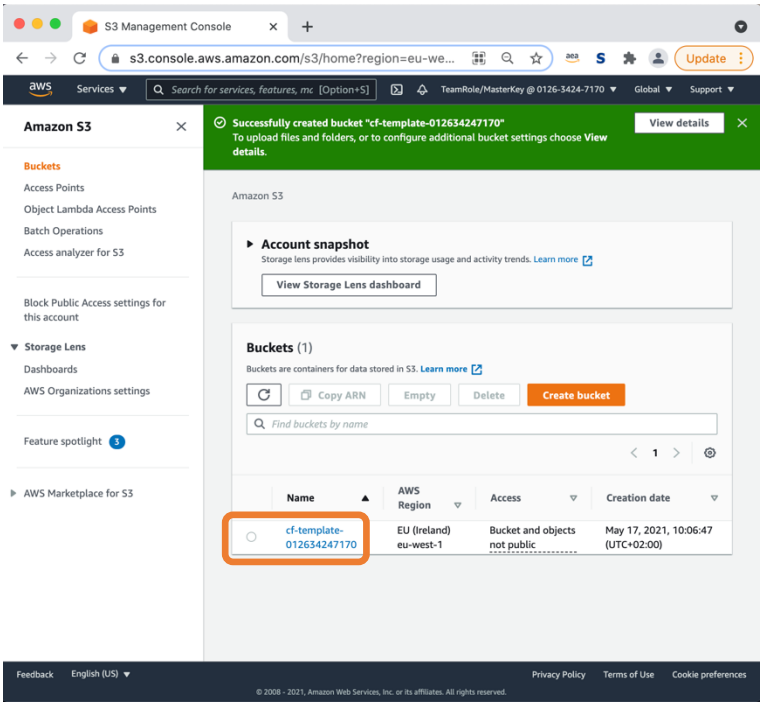
Wybierz polecenie **Create bucket**



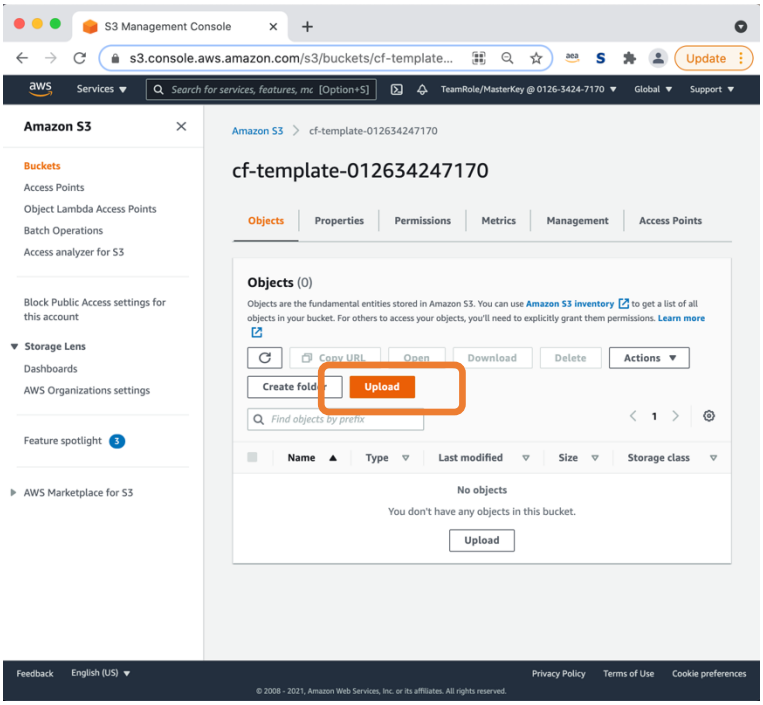
Podaj nazwę koszyka, zweryfikuj region w którym tworzysz koszyk (w ćwiczeniu wybieramy region w Irlandii) i zaakceptuj wszystkie domyślne ustawienia. Nazwa musi być unikalna, możemy wykorzystać numer konta lub inny losowy ciąg znaków do zapewnienia sobie unikalności.



Otwieramy koszyk.



Wgrywamy skrypty konfiguracyjne wybierając polecenie **Upload**.

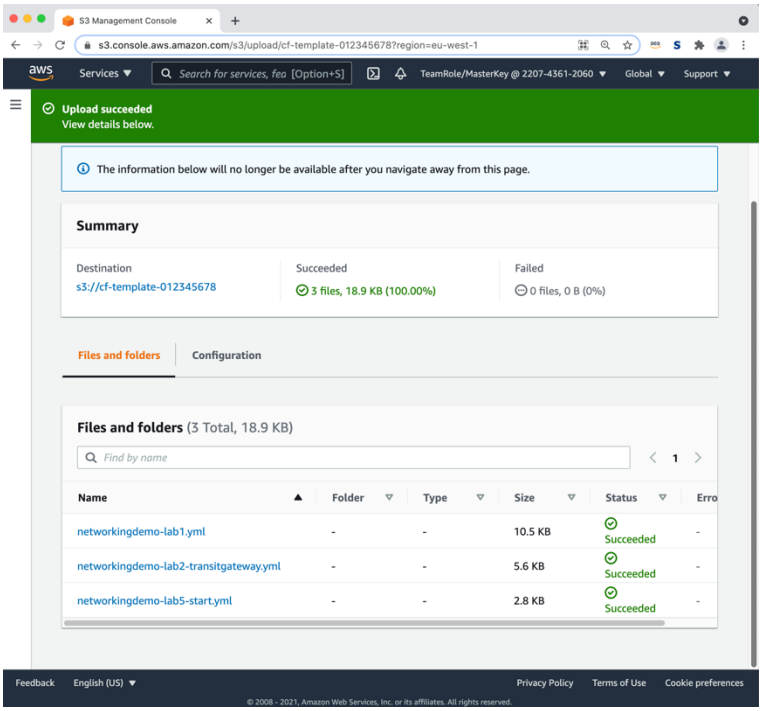


Potrzebujemy następujących skryptów:

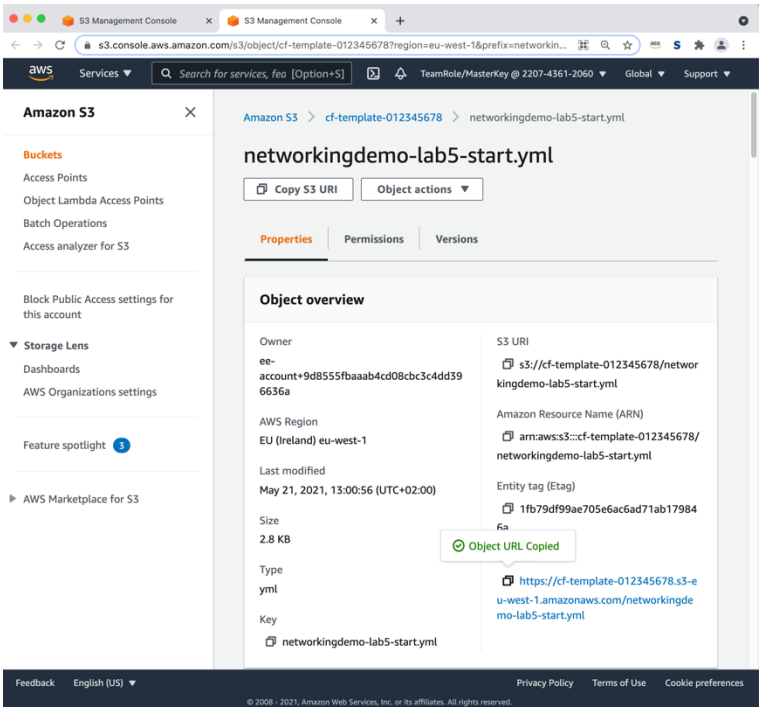
- **`networkingdemo-lab1.yml`** – tworzenie VPC z 4 podsieciami, IGW,NAT Gateway oraz EC2 w prywatnej podsieci;

- **`networkingdemo-lab2-transitgateway.`**yml – tworzenie TGW z podsieciami w 3 VPC;

- **`networkingdemo-lab5-start.yml`** – skrypt łączący wywołanie całości konfiguracji opisanej w powyższych skryptach.

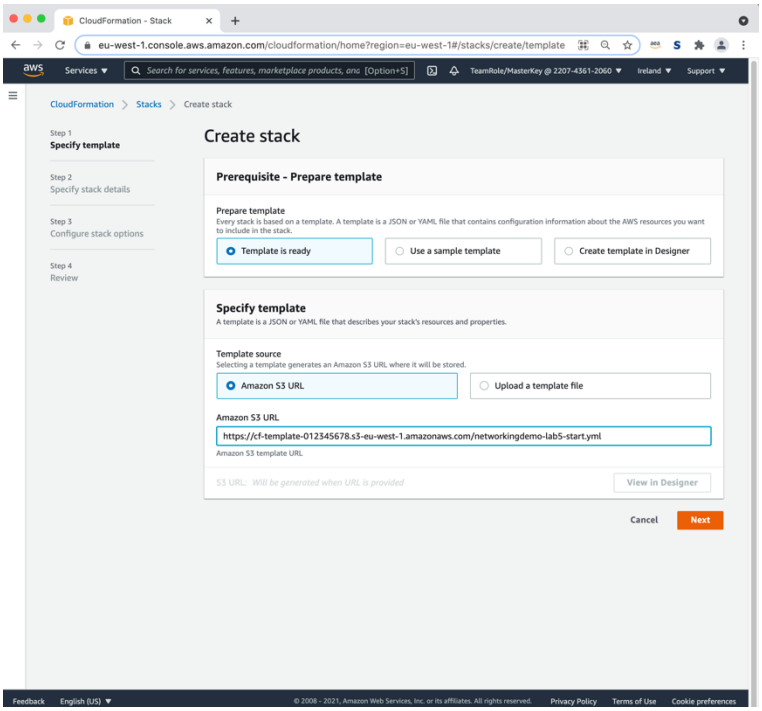


Po wgraniu plików kopiujemy adres URL skryptu startującego **`networkingdemo-lab5-start.yml`**.

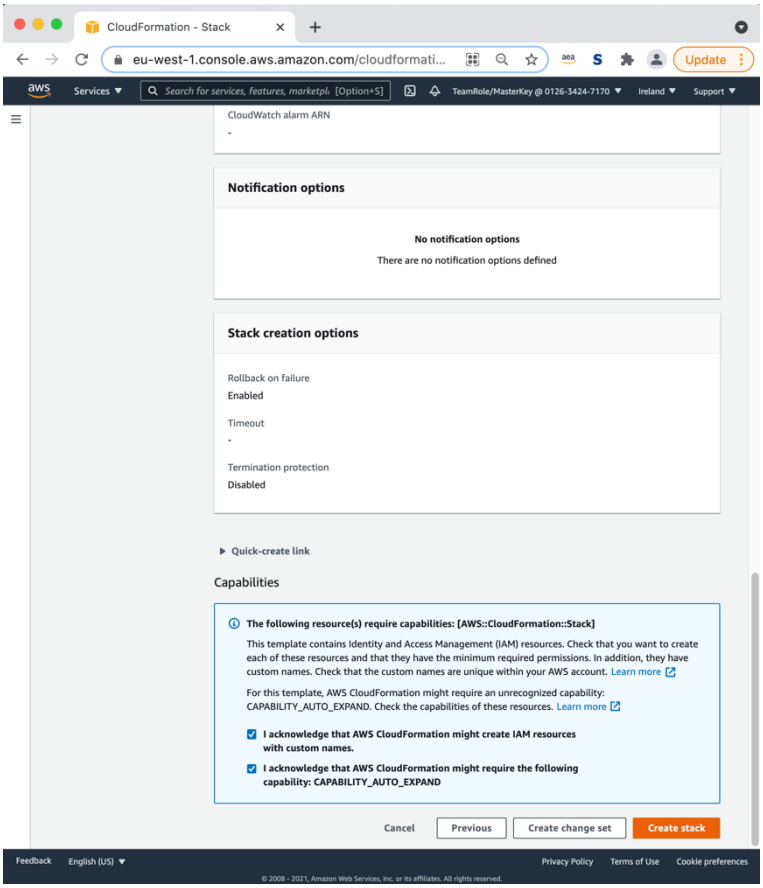


1.3 Utwórz CloudFormation stack z `networkingdemo-lab5-start.yml`

W konsoli AWS wybierz usługę CloudFormation, utwórz stack podając skopiowany adres URL skryptu.



Ciąg BUCKET w adresach URL skryptów zamień na właściwą nazwę koszyka, który utworzyłeś i załadowałeś do niego pliki. Zaakceptuj opcje domyślne.



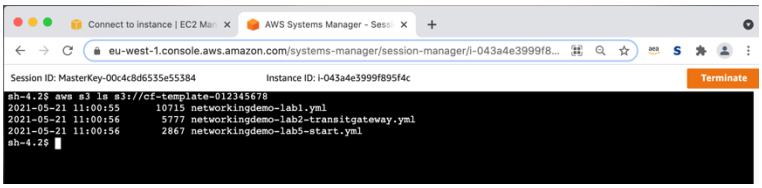
Tworzenie konfiguracji może potrwać około 10 minut.

1.4 Sprawdź komunikację z usługą S3

Wybierz w konsoli AWS usługę EC2. Podłącz się do jednej z maszyn uruchomionych w VPC A lub B lub C korzystając z Session Managera. Teraz jeszcze konfiguracja każdej z maszyn jest analogiczna, wszystkie mają dostęp do internetu.

Użyj polecenia wylistowania wszystkich obiektów w koszyku zamieniając BUCKET_NAME nazwą własnego koszyka (może to być koszyk stworzony na potrzeby skryptów CloudFormation):

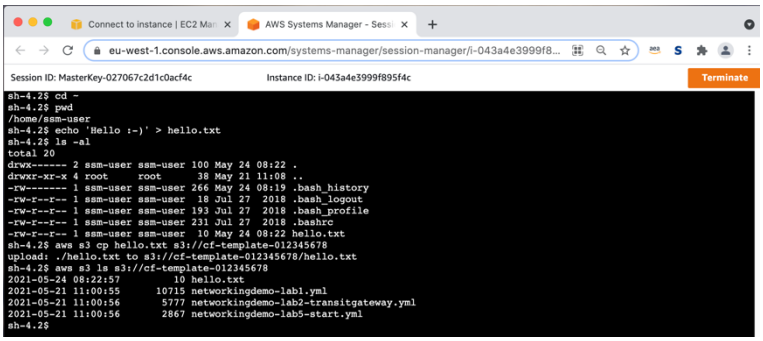
```
aws s3 ls s3://BUCKET_NAME
```



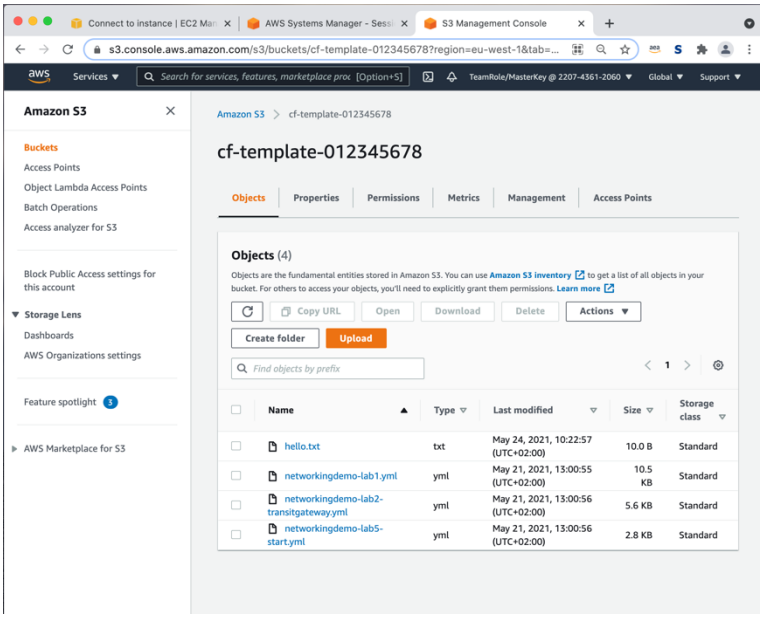

```
echo 'Hello ☺" > hello.txt
```

```
aws s3 cp hello.txt  s3://BUCKET_NAME/
```

```
aws s3 ls s3://BUCKET_NAME/
```



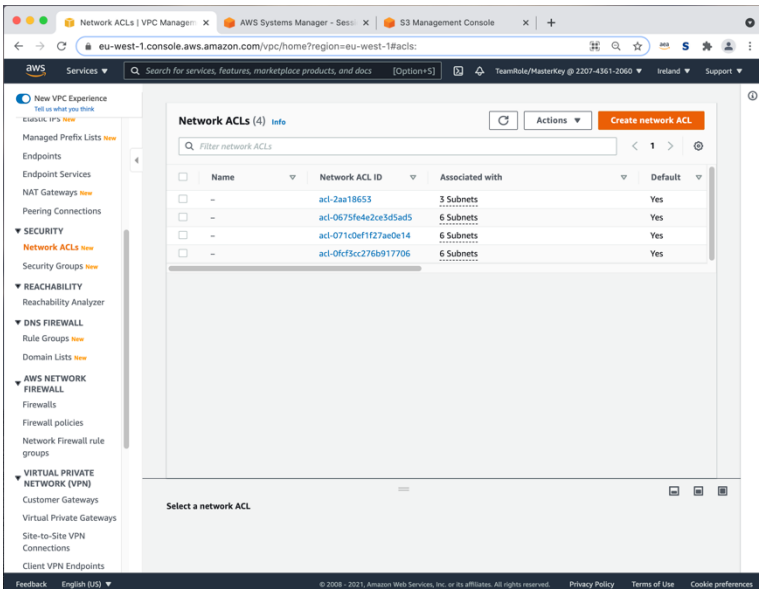
Możesz zweryfikować zawartość koszyka również w konsoli webowej AWS.



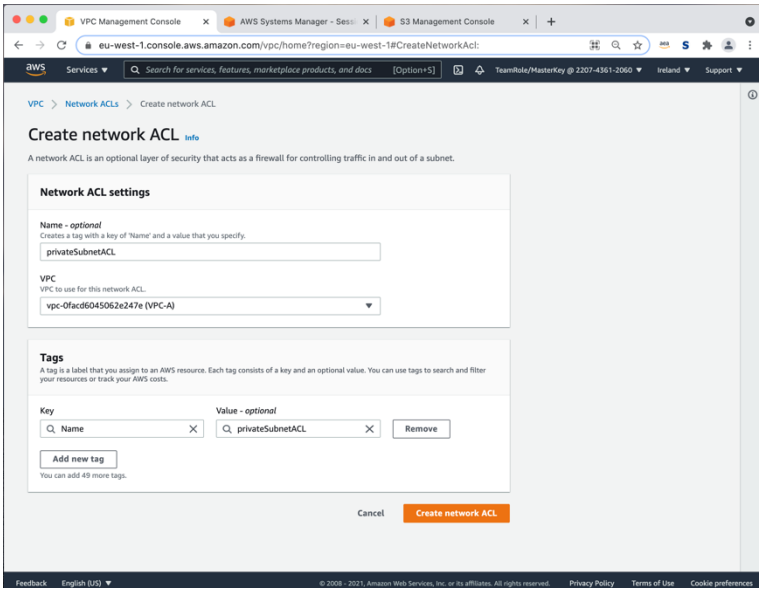
1.5 Zablokuj wyjście z podsieci prywatnej w VPC A do internetu

Dla podsieci w której jest utworzona maszyna w VPC A zdefiniuj ACL, który pozwala wyłącznie na komunikację w lokalnych VPC A, B i C. Zweryfikuj połączenie poprzez Session Manager. Powinieneś utracić możliwość komunikacji z maszyną.

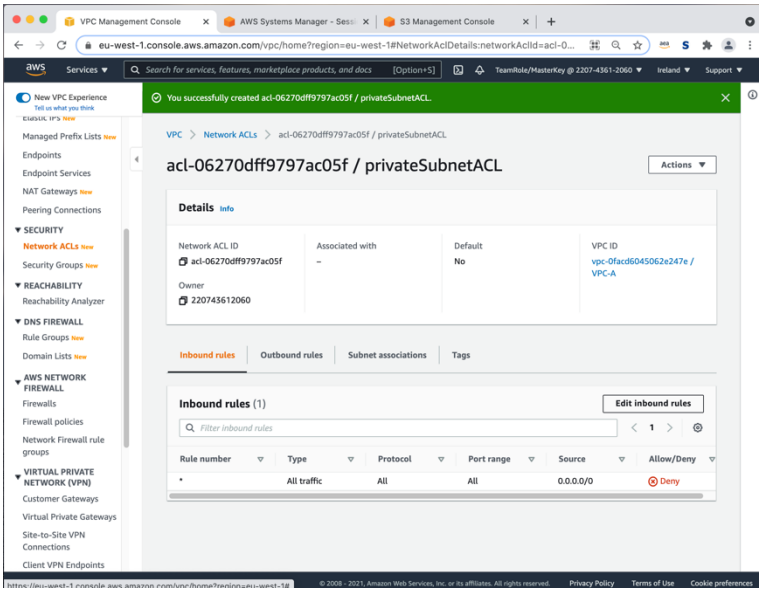
Na stronie usługi VPC z lewego menu wybierz **Network ACLs** i następnie **Create network ACL**.



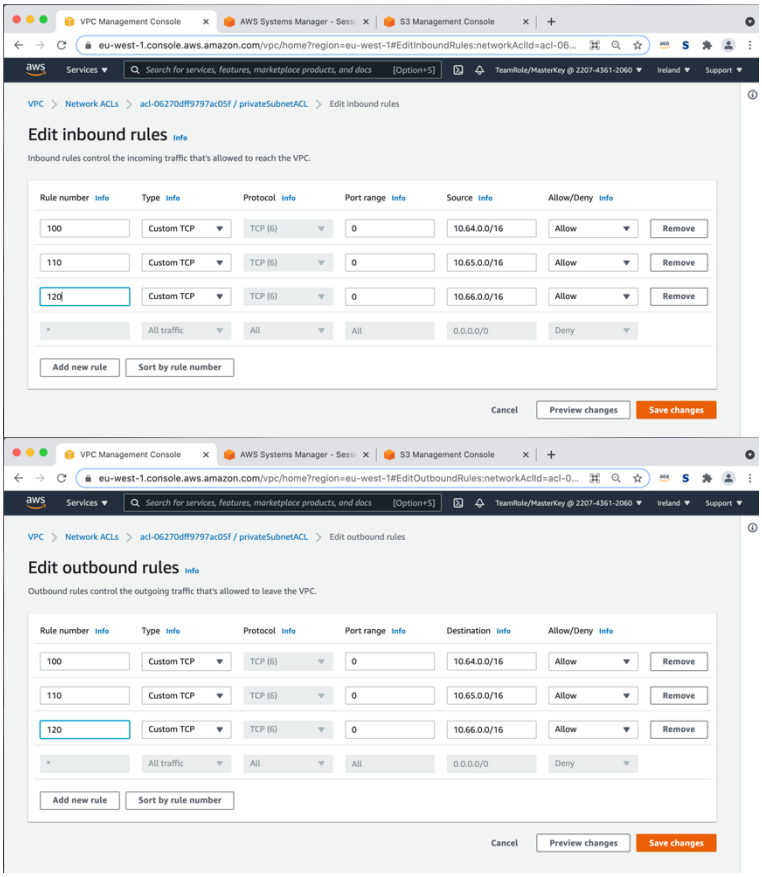
Podaj nazwę dla ACL-ki oraz wybierz VPC-A.



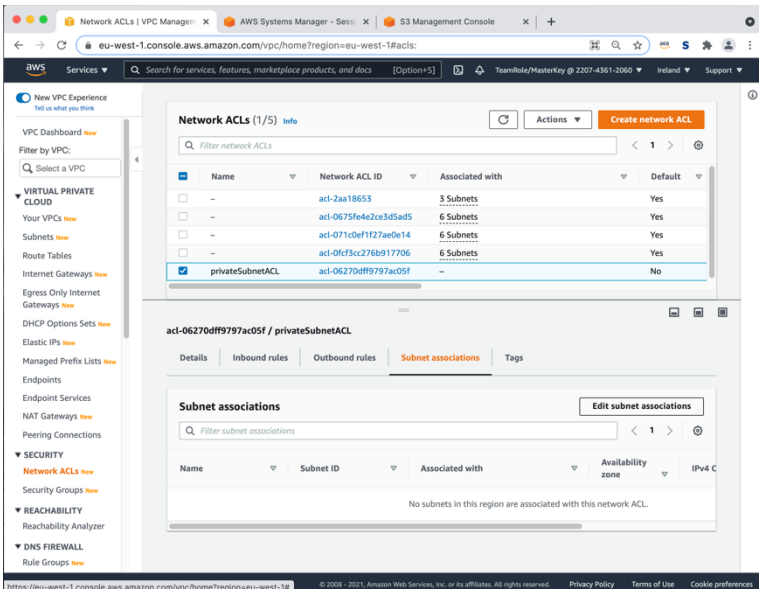
Zauważ, że w odróżnieniu od domyślnego ACL dla VPC nowoutworzona ACL ma tylko regułę blokowania całości ruchu wchodzącego i wychodzącego.



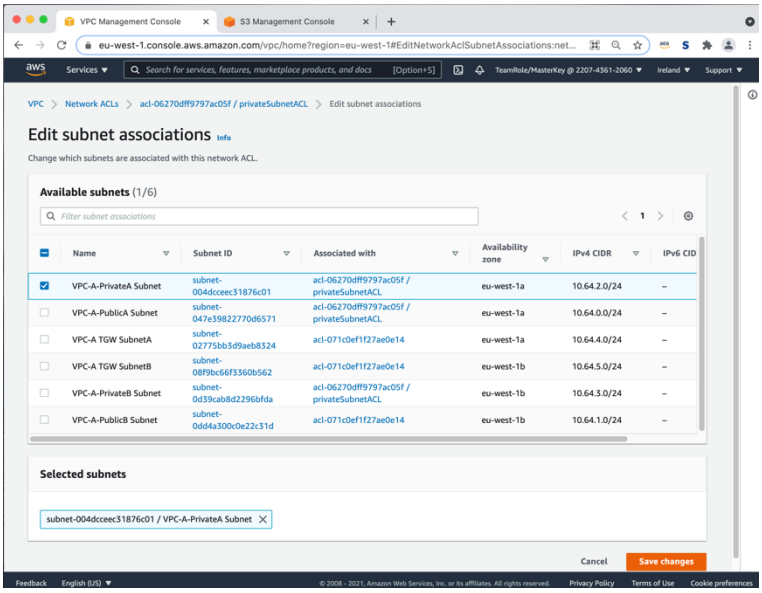
Zdefiniuj ograniczenie ruchu do lokalnych sieci VPC-A, VPC-B oraz VPC-C tak samo dla wchodzącego jak i wychodzącego.

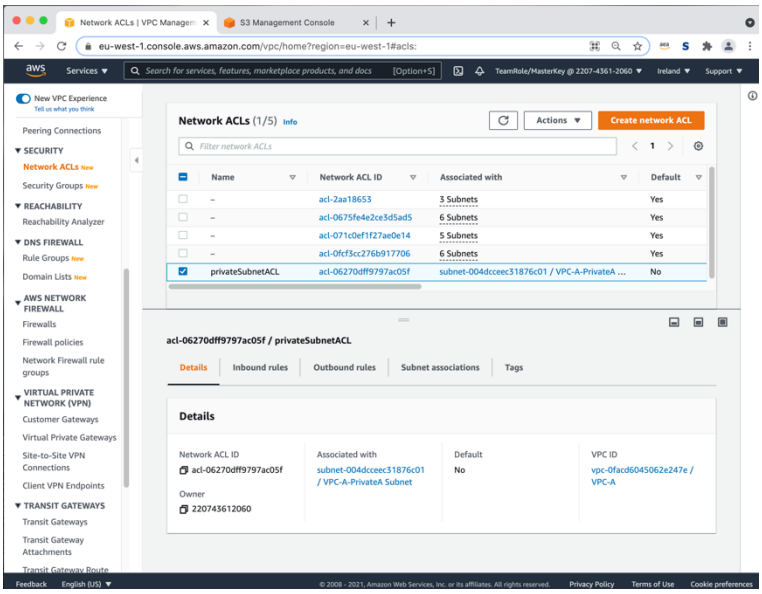


Przypisz nowy ACL do podsieci, której używa maszyna EC2. Przy zaznaczonej ACL wybierz zakładkę **Subnet associations** i polecenie **Edit subnet associations.**



Szukana podsieć to **APC-A-PrivateA Subnet**.

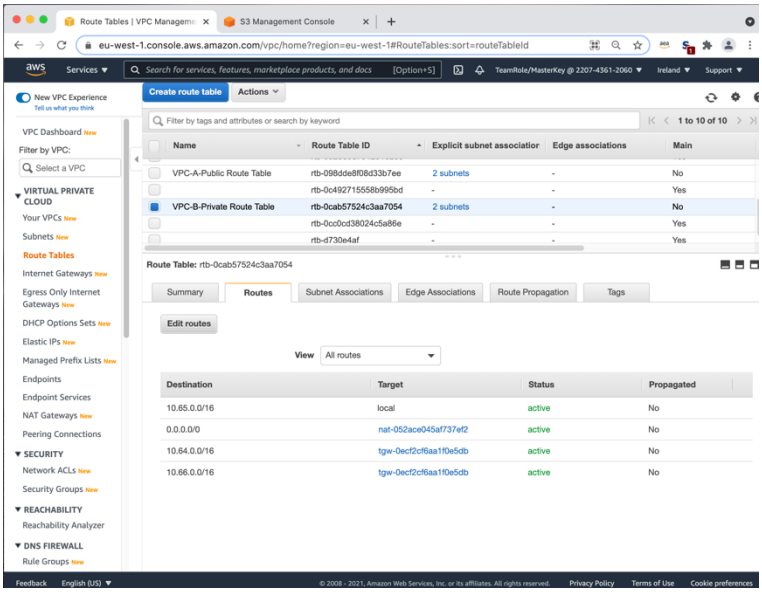


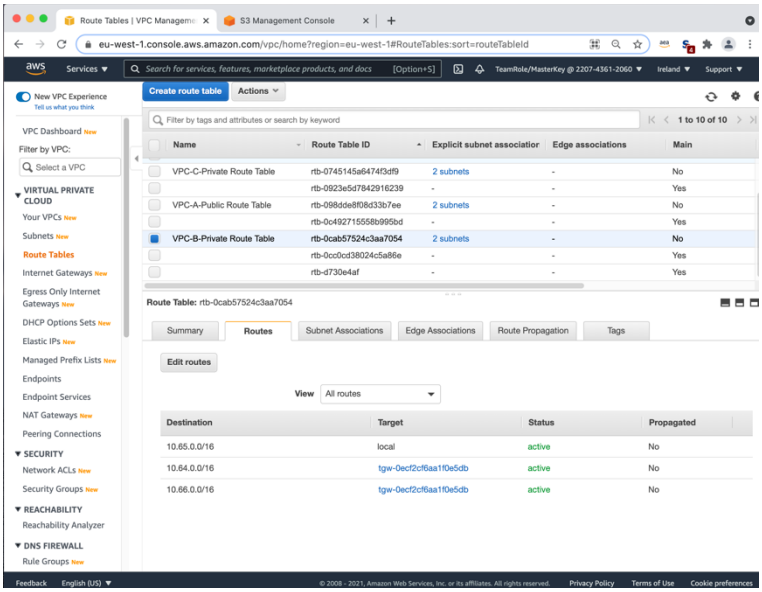


Zweryfikuj połączenie do maszyny. Session Manager powinien teraz być odcięty od maszyny w podsieci z nową ACL. Usługi Session Manager nie są dostępne w lokalnej sieci.

1.6 Zablokuj wyjście z podsieci prywatnej w VPC B do internetu

Dla podsieci w której jest utworzona maszyna w VPC B zmień tablicę routingu, tak by obsłużyć wyłącznie komunikację w lokalnych VPC A, B i C. Utracisz możliwość podłączenia do maszyny z Session Manager'a.

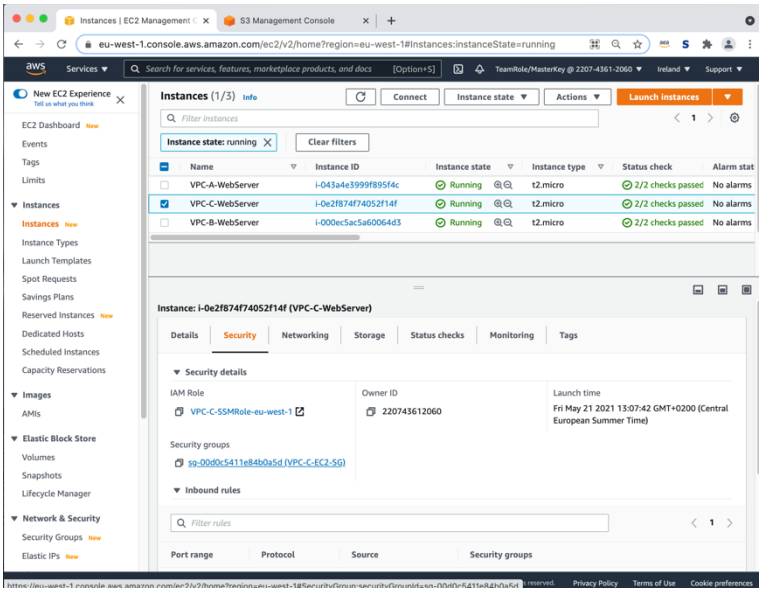




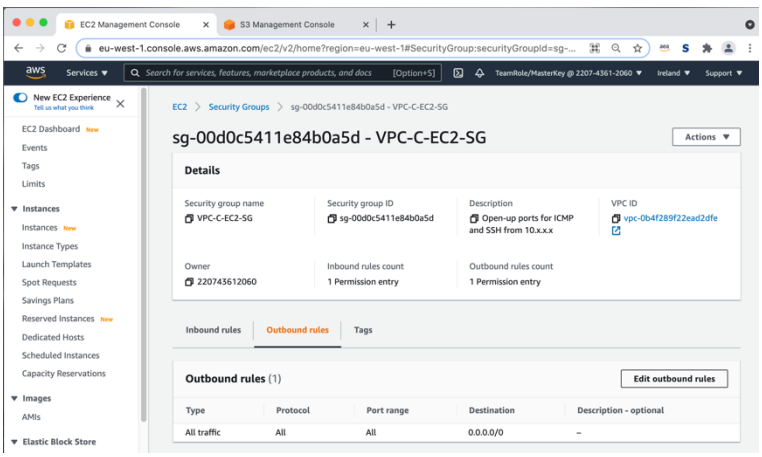
Zweryfikuj, czy dostęp do maszyny został zablokowany.

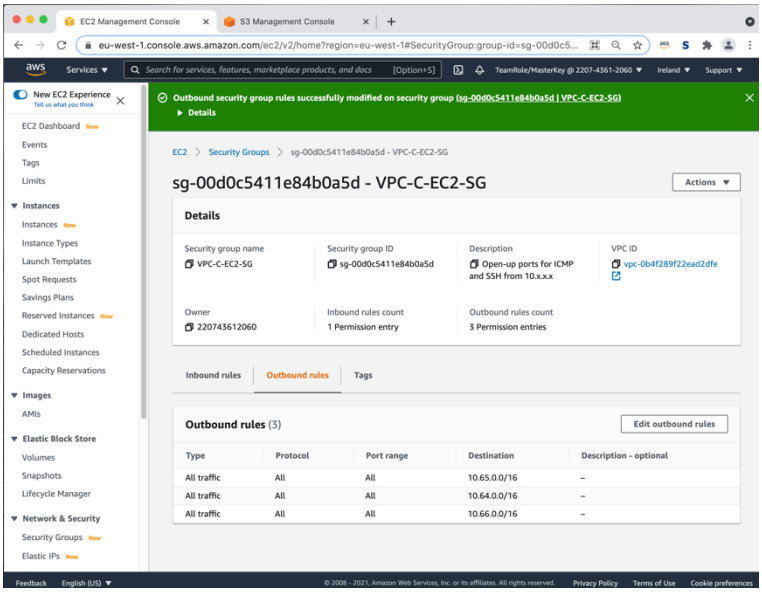
1.7 Zablokuj wyjście z maszyny w VPC C do internetu

Dla maszyny w VPC C zmień definicję security group, tak aby ograniczyć komunikację wyłącznie do sieci z VPC A, B i C. Security groups są dostępne do modyfikacji ze strony usługi EC2, najwygodniej jest przejść do odpowiedniej przez informacje o maszynie wirtualnej EC2.



Modyfikujemy uprawnienia, tak aby ograniczyć ruch wychodzący wyłącznie do lokalnych sieci VPC-A, VPC-B i VPC-C.

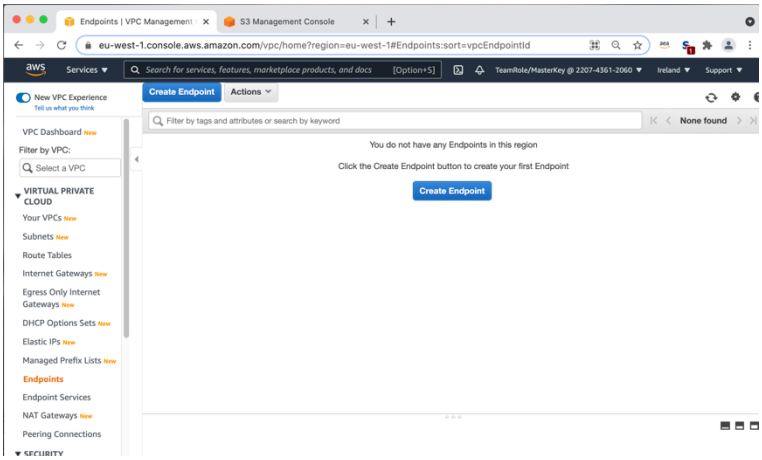




Zweryfikuj efekt działania tej konfiguracji.

1.8 Skonfiguruj endpoint w VPC B dla Systems Manager

Z lewego menu na stronie usługi VPC wybierz **Endpoints** i polecenie **Create Endpoint**.

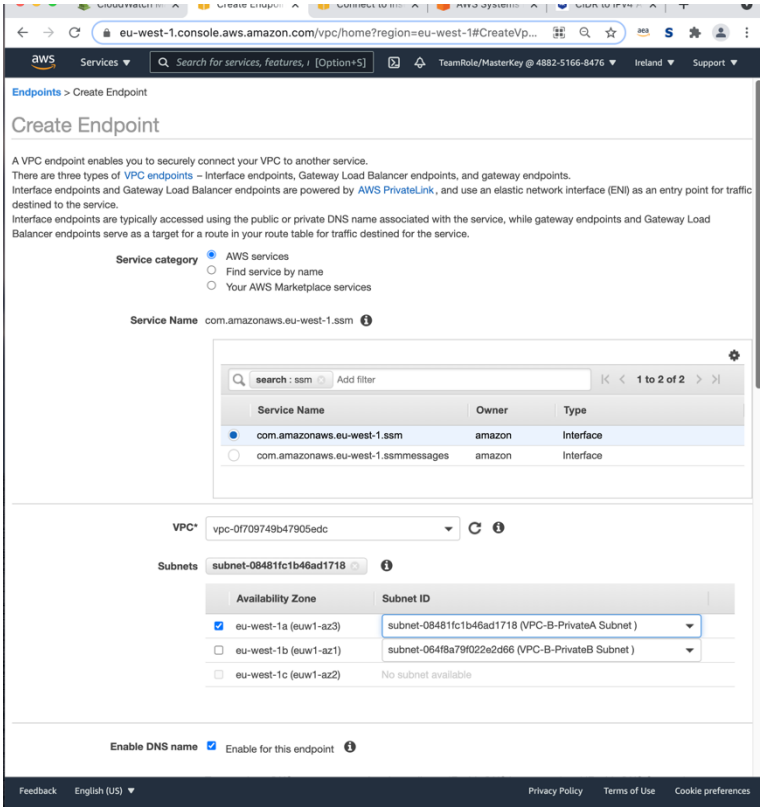


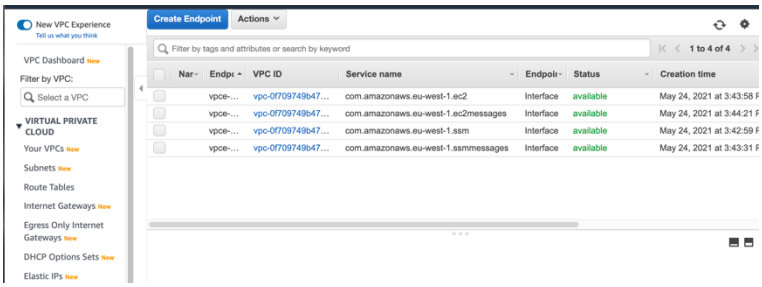
Systems Manager, aby umożliwić swoje usługi potrzebuje 4 interfejsów:

- `com.amazonaws.eu-west-1.ec2`
- `com.amazonaws.eu-west-1.ec2messages`
- `com.amazonaws.eu-west-1.ssm`
- `com.amazonaws.eu-west-1.ssmmessages`

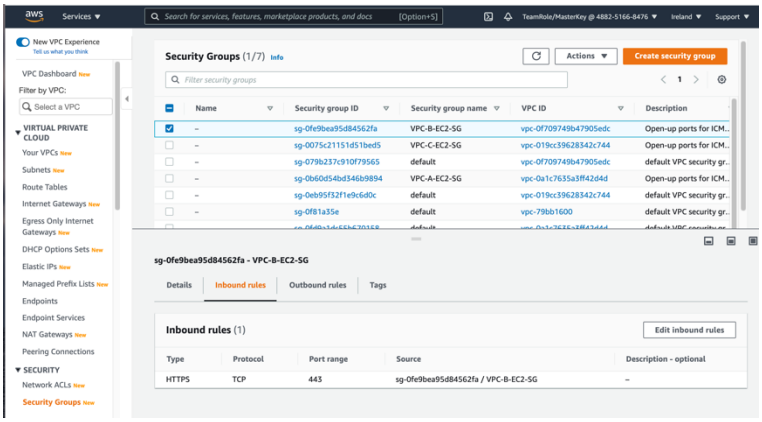
Każdy z interfejsów utwórz w ten sam sposób wybierając:

- **VPC-B**
- Podsieć **VPC-B PrivateA Subnet**
- Security group **VPC-B-EC2-SG**





Dla security group **VPC-B-EC2-SG** ustaw możliwość odbierania komunikacji po HTTPS. Interfejsy Session Manager są wywoływane przez agenta działającego na maszynie EC2 na porcie 443.



Kiedy wszystkie 4 interfejsy będą dostępne możesz zweryfikować, czy mimo braku komunikacji z Internetem maszyna jest dostępna przez SessionManager.

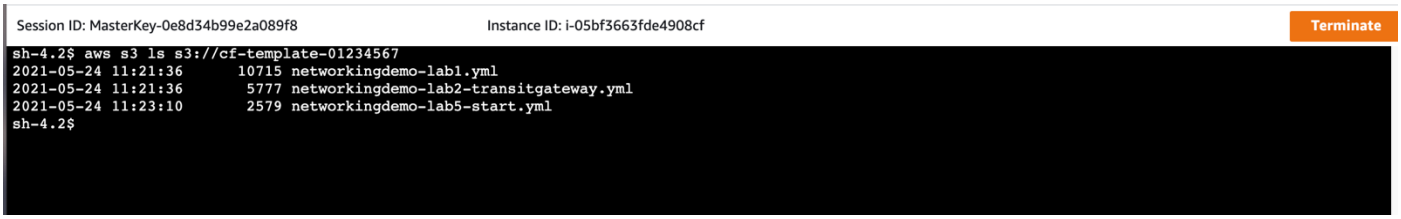
1.9 Skonfiguruj endpoint w VPC B dla SNS i S3

Na takiej samej zasadzie są udostępniane dla sieci prywatnych inne usługi AWS. W tym kroku użyjemy usługi SNS i S3.

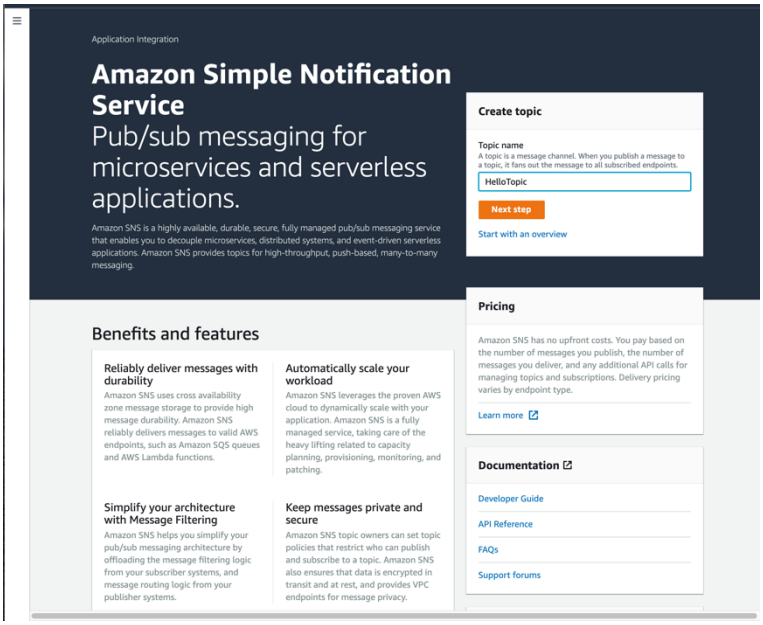
Dla usługi S3 stwórz com.amazonaws.eu-west-1.s3 gateway wskazując tablicę routowania podpiętą dla podsieci **VPC-B PrivateA Subnet.**

Zweryfikuj, czy komunikacja z usługą S3 działa:

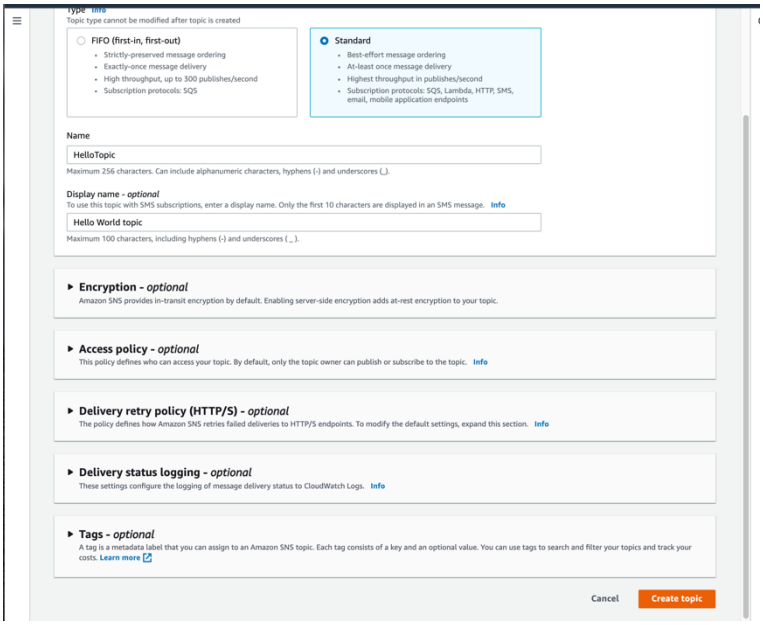
```
aws s3 ls s3://BUCKET_NAME/
```

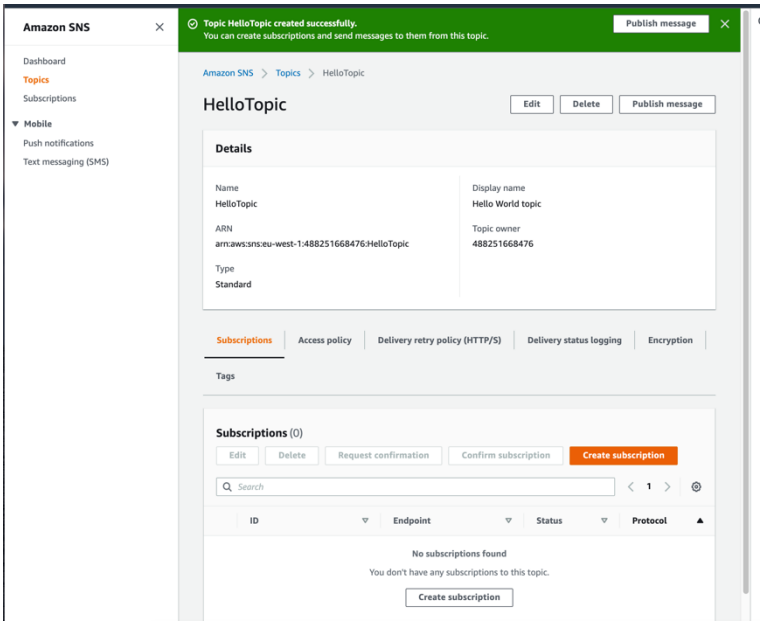


Stwórz interfejs dla usługi com.amazonaws.eu-west-1.sns. Nie czekając na uaktywnieni się interfejsu, przejdź do konfiguracji usługi SNS, wybierając ją w wyszukiwarce usług w konsoli AWS.



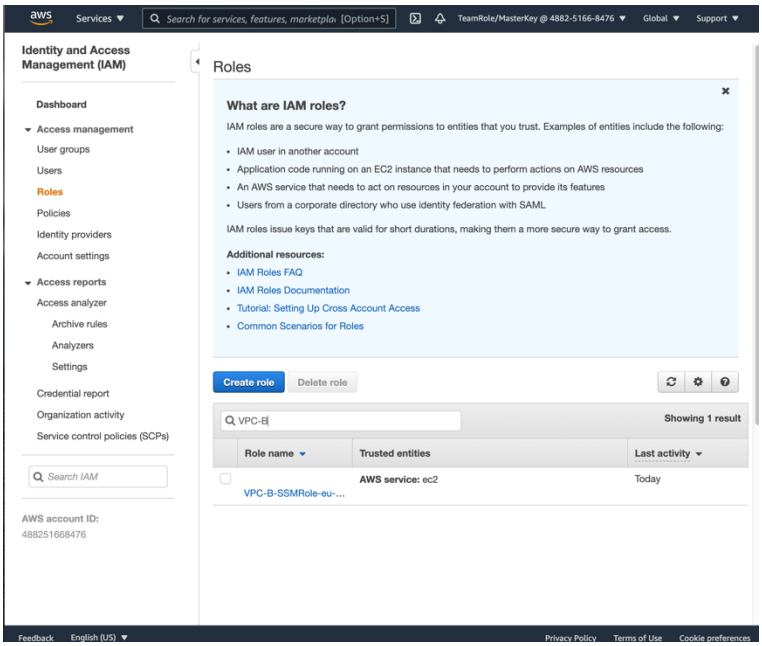
Podaj nazwę **Topic**, na który będziemy wysyłać powiadomienia i wybierz standardowy model komunikacji (nie gwarantuje kolejności dostarczenia wiadomości).



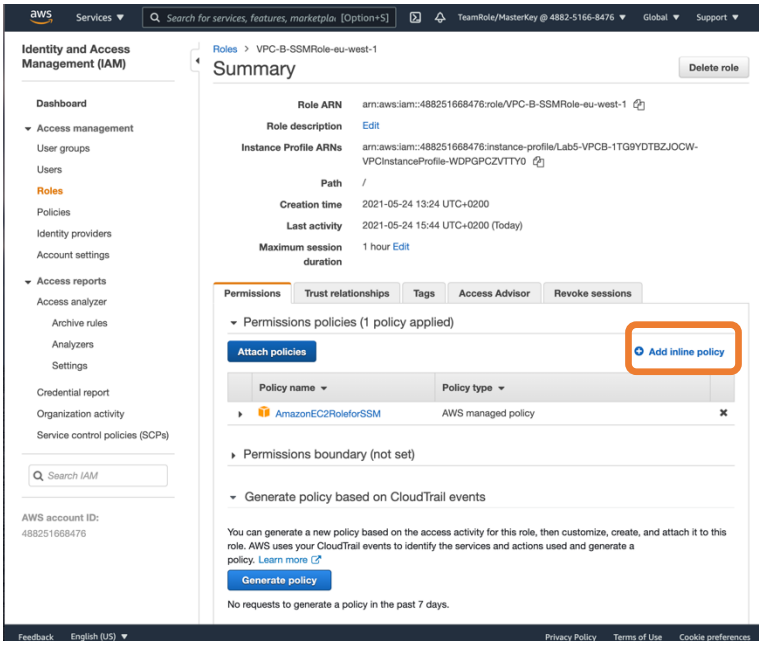


Dodaj subskrypcję na SMS lub email, tak aby odebrać faktycznie powiadomienie.

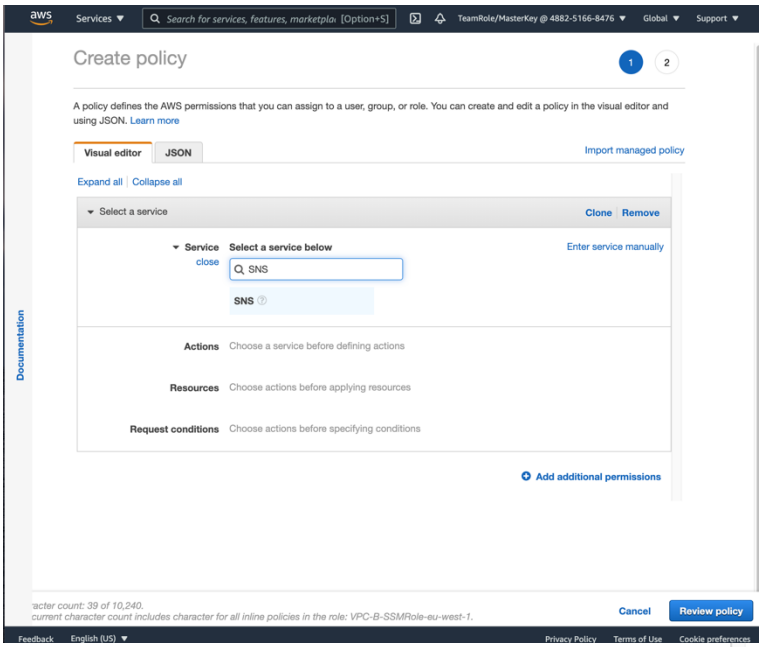
Teraz zmodyfikuj uprawnienia roli na jakiej działa maszyna EC2, tak żeby możliwe było wysłanie wiadomości poleceniem z maszyny. Na stronie usługi **IAM**, wybierz **Roles** i wyszukaj roli o nazwie zaczynającej się od **VPC-B**.

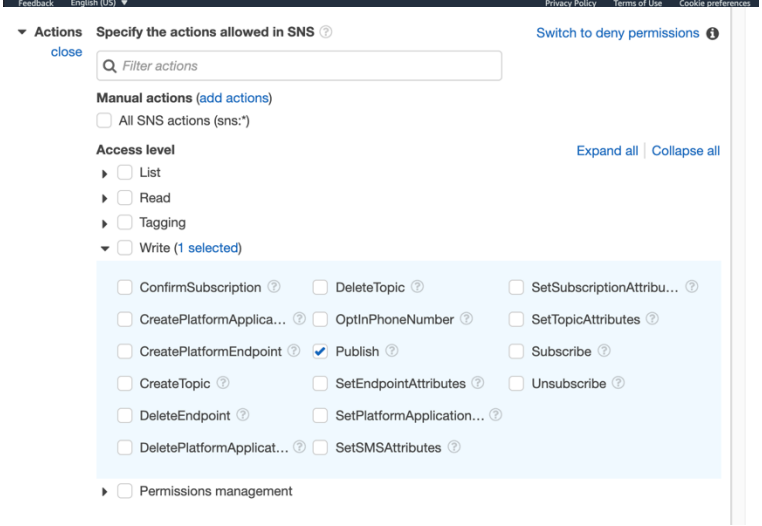


Dla tej roli dodaj inline policy.

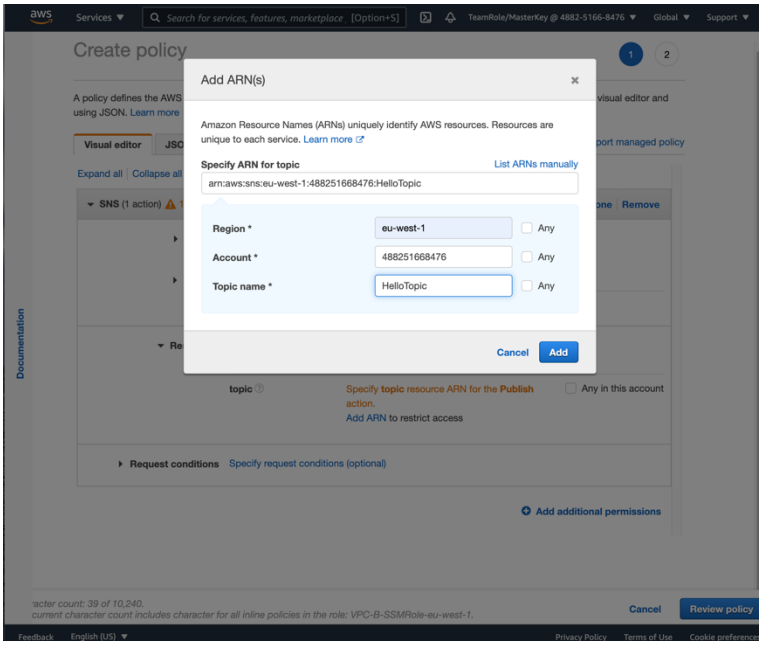


Otworzy się wizualny edytor uprawnień. Wybierz usługę SNS, następnie jako jedyną akcję Publish.

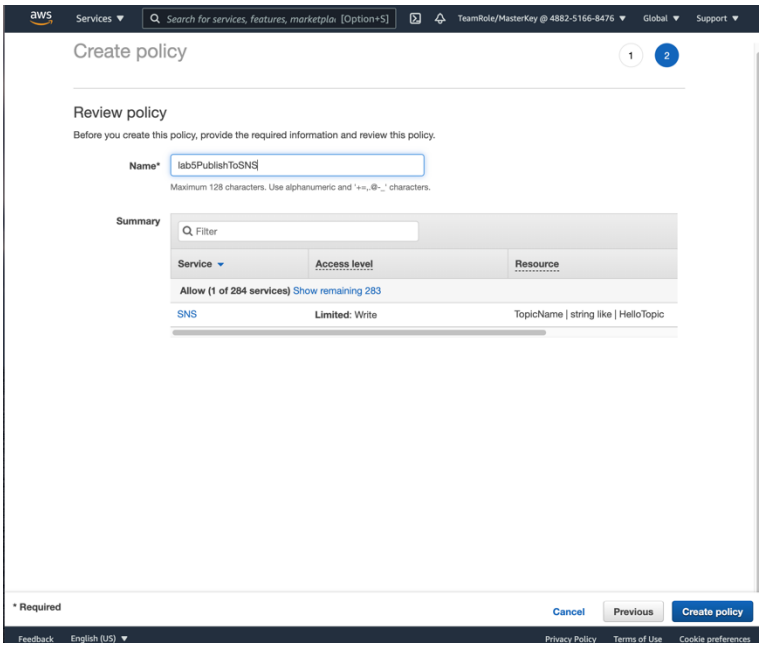


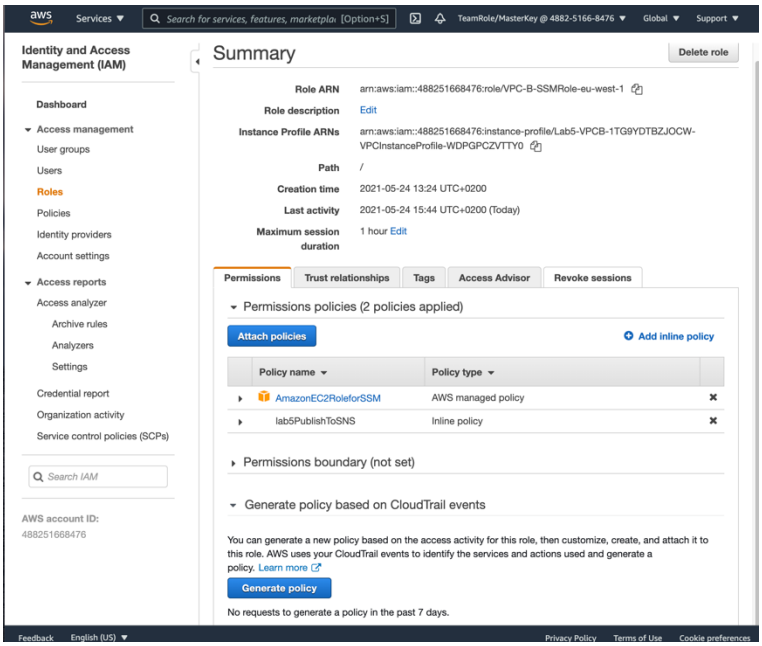


Ogranicz uprawnienia publikowania wiadomości do konkretnego zasobu podając region oraz nazwę Topic'u.



Nadaj nazwę tej regule i ją zapisz. To zmodyfikowało uprawnienia maszyny.

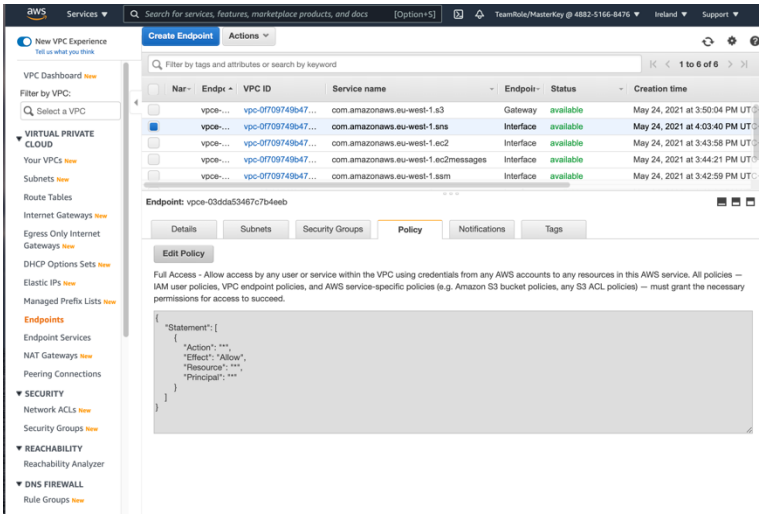




Sprawdź komunikację z usługą SNS wywołując polecenie po podstawieniu pod `sns-topic-arn` właściwego identyfikatora tematu:

```
aws sns publish --region eu-west-1 --topic-arn sns-topic-arn --message "Hello ☺"
```

Usługa działa, ale naraziliśmy się na dostawanie wiadomości typu „Hello”. Teraz zmodyfikuj zakres uprawnień jaki ma interfejs SNS wystawiony w VPC-B. W zakładce Policy dla zaznaczonego interfejsu SNS wybierz **Edit Policy**. Możesz wykorzystać generator uprawnień, lub poniżej załączony szablon, który wyklucza możliwość wysłania wiadomości ze słowem „Hello” w treści.




```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sns:Publish"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:sns:eu-west-1:488251668476:HelloTopic",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/Message": "*Hello*"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Sprawdź, czy teraz wiadomość z tekstem hello nie może być wysłana.

```
sh-4.2$ aws sns publish --region eu-west-1 --topic-arn arn:aws:sns:eu-west-1:488251668476:HelloTopic --message "Hello world"

An error occurred (AuthorizationError) when calling the Publish operation: User: arn:aws:sts::488251668476:assumed-role/VPC-B-SSMRole-eu-wes
t-1/i-05bf3663fde4908cf is not authorized to perform: SNS:Publish on resource: arn:aws:sns:eu-west-1:488251668476:HelloTopic
sh-4.2$ aws sns publish --region eu-west-1 --topic-arn arn:aws:sns:eu-west-1:488251668476:HelloTopic --message "Czesc :-)"
{
    "MessageId": "8d93ced3-0f61-5567-a20b-97f6c14adce8"
}
sh-4.2$
```

Ukończyłeś ćwiczenie!