Bezpieczne systemy rozproszone(firma bankowa)

Mikita Shmyhaliou 259073
Rafał Dżendżera 253011

Politechnika Wrocławska

27.06.2023

Spis treści

1 Introduction

Działalność banku obejmuje prowadzenie kont i lokat, udzielanie kredytów, wykonywanie przelewów, wypłatę gotówki, udostępnianie kart, a także sprzedaż ubezpieczeń. Bank posiada własną stronę internetową oraz aplikację na telefon. W ramach działalności przechowywane są różne rodzaje danych, w tym informacje o klientach, dane finansowe, dane dotyczące pożyczek i kredytów, dane inwestycyjne i dane ubezpieczeniowe.

2 Założenia projektowe

Planujemy, że firma będzie cechować się:

1. bezpieczeństwem i zgodnością ze standardami bezpieczeństwa
2. wysoką dostępnością
3. wysoką skalowalnością
4. analityką danych, która pomaga przetwarzać i analizować duże ilości danych z różnych źródeł, umożliwiając wgląd w zachowania, preferencje i trendy klientów.

3 Zastosowane usługi

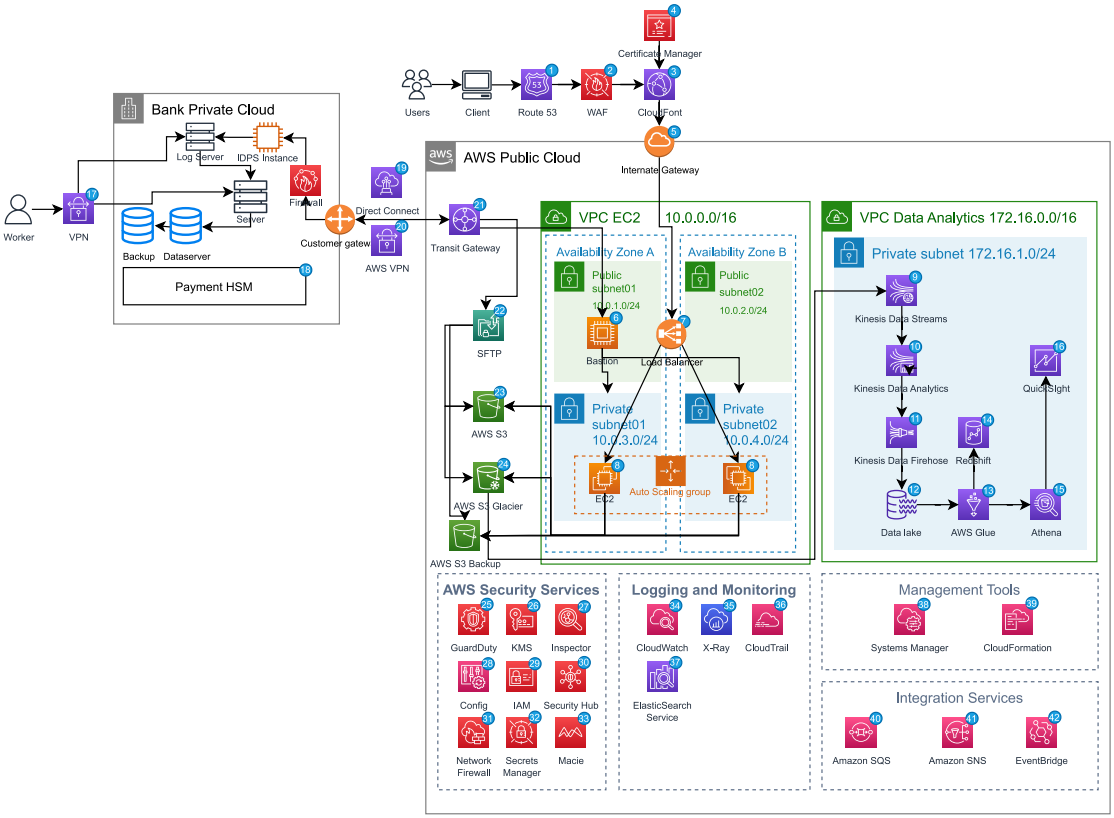
Private cloud services

1. Wrażliwe dane klientów
2. Przechocwywanie danych firmowych
3. Zapewnienie bezpieczeństwa
4. Historia bankowa klientów
5. Infrastruktura sieciowa
6. Backup
7. Uczenie maszynowe

Public cloud services

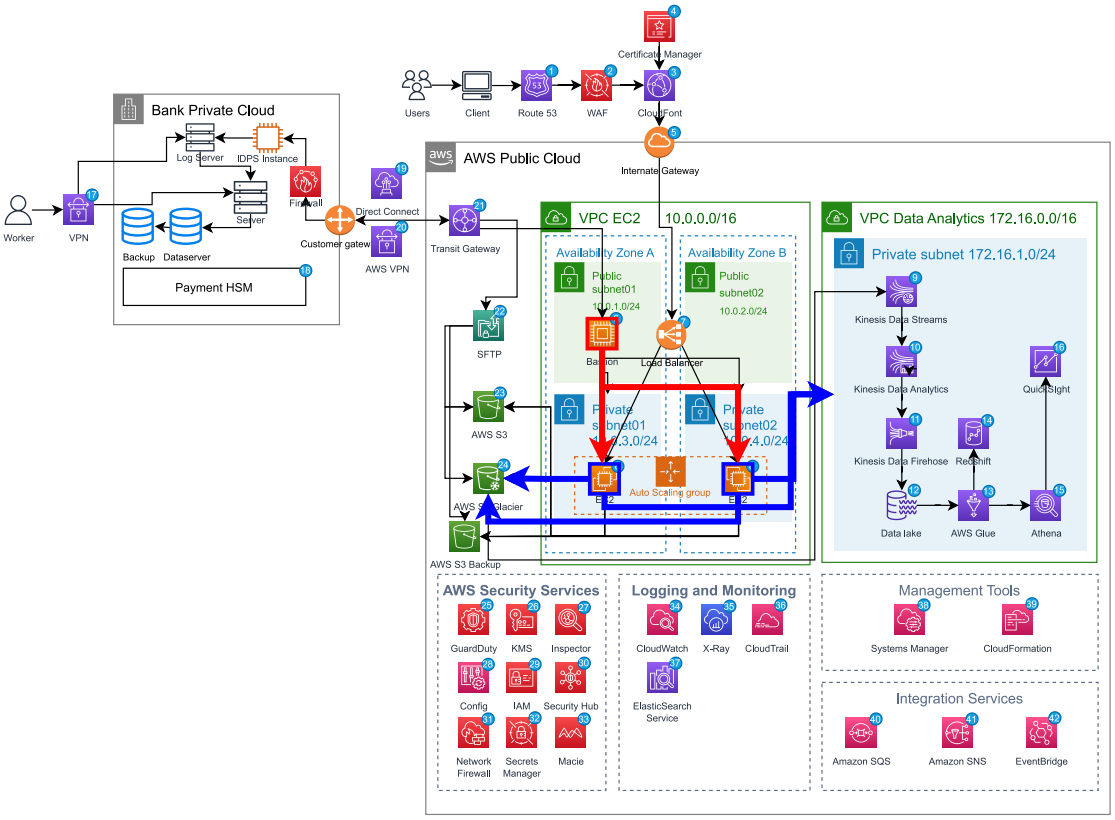
1. Bankowość internetowa i mobilna
2. Analityka danych
3. Marketing
4. Dane na temat usług banku
5. Dane o placówkach
6. Komunikacja
7. CDN
8. Uczenie maszynowe

4 Schemat AWS



Rysunek 1: AWS schema

5 Schemat AWS (Security Groups)



Rysunek 2: AWS security groups

6 Opis schemata

1. Route 53 to wysoko skalowalna i niezawodna usługa sieciowa systemu nazw domen (DNS) dostarczana przez AWS. Umożliwia zarządzanie nazwami domen (takimi jak example.com) i powiązanymi rekordami DNS (takimi jak A, CNAME, MX itp.), które są niezbędne do kierowania ruchu do zasobów. Route 53 jest powszechnie używany do rejestracji domen, zarządzania DNS i kierowania przychodzących żądań użytkowników do odpowiednich zasobów w ramach infrastruktury. Oferuje funkcje takie jak kontrole kondycji, zasady routingu ruchu i globalne równoważenie obciążenia, aby zapewnić wysoką dostępność i wydajność aplikacji.

2. WAF to usługa bezpieczeństwa świadczona przez AWS, która pomaga chronić aplikacje internetowe przed typowymi exploitami i atakami internetowymi. Działa jako filtr między aplikacją internetową a ruchem przychodzącym, sprawdzając żądania i blokując potencjalnie złośliwy ruch.

3. CloudFront to usługa content delivery network (CDN) świadczona przez Amazon Web Services (AWS). Została zaprojektowana w celu dostarczania treści, w tym stron internetowych, filmów, obrazów i innych statycznych lub dynamicznych plików, do użytkowników z niskim opóźnieniem i dużą prędkością transferu danych. CloudFront działa poprzez buforowanie i serwowanie treści z lokalizacji brzegowych zlokalizowanych na całym świecie, bliżej użytkowników żądających treści.

4. Certificate Manager to usługa świadczona przez Amazon Web Services (AWS), która ułatwia dostarczanie, zarządzanie i wdrażanie certyfikatów SSL/TLS (Secure Sockets Layer/Transport Layer Security) do użytku z usługami AWS i aplikacjami.

5. Internat Gateway (IGW) to skalowalna poziomo, wysoko dostępna usługa AWS, która umożliwia komunikację między wirtualną chmurą prywatną Amazon (Amazon VPC) a Internetem. Działa jako brama ułatwiająca ruch przychodzący i wychodzący między VPC a publicznym Internetem.

6. Host Bastion to instancja EC2, która jest bezpiecznie skonfigurowana w celu zezwalania na przychodzące połączenia Secure Shell (SSH) z

określonych adresów IP lub zakresów IP. Działa jako bezpieczny punkt wejścia dla administratorów, aby uzyskać dostęp do innych instancji lub zasobów w prywatnej podsieci wirtualnej chmury prywatnej (VPC).

7. W AWS Load Balancer to zarządzana usługa, która pomaga dystrybuować przychodzący ruch sieciowy między wieloma instancjami lub zasobami, aby zapewnić wysoką dostępność, odporność na błędy i skalowalność aplikacji.

8. Amazon Elastic Compute Cloud (EC2) to usługa internetowa świadczona przez Amazon Web Services (AWS), która umożliwia udostępnianie i zarządzanie serwerami wirtualnymi, zwanymi instancjami, w chmurze. EC2 zapewnia skalowalne zasoby obliczeniowe, umożliwiając szybkie skalowanie w górę lub w dół w zależności od wymagań aplikacji.

9. Amazon Kinesis Data Streams to w pełni zarządzana usługa dostarczana przez Amazon Web Services (AWS), która umożliwia gromadzenie, przetwarzanie i analizowanie danych strumieniowych w czasie rzeczywistym. Jest ona przeznaczona dla aplikacji i przypadków użycia, które wymagają obsługi dużych ilości ciągłych danych strumieniowych z różnych źródeł, takich jak strumienie kliknięć na stronie internetowej, urządzenia IoT, dzienniki, kanały mediów społecznościowych i inne.

10. Amazon Kinesis Data Analytics to w pełni zarządzana usługa świadczona przez Amazon Web Services (AWS), która umożliwia przetwarzanie i analizowanie danych strumieniowych w czasie rzeczywistym przy użyciu standardowych zapytań SQL. Upraszcza to zadanie pisania złożonego kodu lub zarządzania infrastrukturą do analizy danych strumieniowych w czasie rzeczywistym.

11. Amazon Kinesis Data Firehose to w pełni zarządzana usługa świadczona przez Amazon Web Services (AWS), która umożliwia przechwytywanie, przekształcanie i ładowanie danych strumieniowych do pamięci masowej i usług analitycznych bez konieczności ręcznego kodowania lub zarządzania infrastrukturą. Upraszcza ona proces pozyskiwania i dostarczania danych strumieniowych w czasie rzeczywistym.

12. Data Lake to scentralizowane repozytorium, które umożliwia przechowywanie ustrukturyzowanych, częściowo ustrukturyzowanych i nieustrukturyzowanych danych w dowolnej skali. Zostało zaprojektowane do prze-

chowywania nieprzetworzonych danych w ich oryginalnej formie, bez potrzeby wcześniejszego definiowania schematu lub transformacji danych. Koncepcja jeziora danych polega na gromadzeniu i przechowywaniu danych z różnych źródeł, umożliwiając elastyczną i skalowalną analizę, eksplorację i przetwarzanie.

13. AWS Glue to w pełni zarządzana usługa ekstrakcji, transformacji i ładowania (ETL) świadczona przez Amazon Web Services (AWS). Upraszcza ona proces przygotowywania i przekształcania danych na potrzeby analityki, uczenia maszynowego i innych zadań przetwarzania danych. Glue pomaga zautomatyzować czasochłonne zadania odkrywania danych, katalogowania danych i transformacji danych, ułatwiając tworzenie i utrzymywanie potoków danych.

14. Amazon Redshift to w pełni zarządzana usługa hurtowni danych w skali petabajtów świadczona przez Amazon Web Services (AWS). Została zaprojektowana do obsługi dużych obciążeń analitycznych i zapewnia wysoką wydajność zapytań na ogromnych zbiorach danych. Redshift oferuje kolumnowy format przechowywania danych, równoległe wykonywanie zapytań i automatyczne skalowanie w celu dostarczania szybkich i skalowalnych rozwiązań analitycznych.

15. Amazon Athena to interaktywna usługa zapytań dostarczana przez Amazon Web Services (AWS), która umożliwia analizowanie danych bezpośrednio w Amazon S3 przy użyciu standardowych zapytań SQL. Jest to usługa bezserwerowa, co oznacza, że nie trzeba dostarczać ani zarządzać żadną infrastrukturą. Dzięki Athena można szybko i łatwo wysyłać zapytania i analizować duże ilości danych przechowywanych w S3 bez konieczności stosowania złożonych procesów ładowania lub przekształcania danych.

16. QuickSigth umożliwia użytkownikom łatwe tworzenie interaktywnych pulpitów nawigacyjnych, przeprowadzanie analiz ad-hoc i generowanie wizualizacji z różnych źródeł danych. QuickSight został zaprojektowany tak, aby był szybki, skalowalny i opłacalny, umożliwiając organizacjom uzyskiwanie wglądu w dane i podejmowanie decyzji opartych na danych.

17. VPN (Virtual Private Network) umożliwia ustanowienia bezpiecznego i

szyfrowanego połączenia między siecią lokalną lub urządzeniami klienckimi a zasobami AWS

18. Payment HSM to wzmocnione, odporne na manipulacje urządzenie sprzętowe, które jest używane w celu zapewnienia wysokiego poziomu ochrony kluczy kryptograficznych i kodów PIN klientów używanych podczas wydawania kart z paskiem magnetycznym i chipem EMV (oraz ich odpowiedników w aplikacjach mobilnych), a następnie przetwarzania transakcji płatniczych kartami kredytowymi i debetowymi. Płatnicze moduły HSM zwykle zapewniają natywne wsparcie kryptograficzne dla wszystkich głównych aplikacji płatniczych systemów kartowych i przechodzą rygorystyczną niezależną certyfikację sprzętu w ramach globalnych programów, takich jak FIPS 140-2, PCI HSM i innych dodatkowych regionalnych wymogów bezpieczeństwa, takich jak MEPS we Francji i APCA w Australii.

19. AWS Direct Connect to usługa sieciowa świadczona przez Amazon Web Services (AWS), która umożliwia ustanowienie dedykowanego i prywatnego połączenia między siecią lokalną a AWS. Zapewnia połączenie o wysokiej przepustowości i niskich opóźnieniach, które omija publiczny Internet, oferując bardziej niezawodne i bezpieczne połączenie w celu uzyskania dostępu do zasobów AWS.

20. VPN (Virtual Private Network) umożliwia ustanowienia bezpiecznego i szyfrowanego połączenia między siecią lokalną lub urządzeniami klienckimi a zasobami AWS

21. AWS Transit Gateway to w pełni zarządzana usługa świadczona przez Amazon Web Services (AWS), która upraszcza łączność i routing między wieloma wirtualnymi chmurami prywatnymi (VPC), sieciami lokalnymi i bramami AWS Direct Connect. Działa jako hub, który pozwala konsolidować i kontrolować ruch sieciowy między różnymi sieciami w ramach infrastruktury AWS.

22. AWS udostępnia usługę o nazwie AWS Transfer for SFTP (Simple File Transfer Protocol), która umożliwia konfigurowanie i zarządzanie bezpiecznymi transferami plików przy użyciu protokołu SFTP. Oferuje ona w pełni zarządzane rozwiązanie do przesyłania plików do i z pamięci masowej Amazon S3 lub Amazon Elastic File System (EFS).

23. Amazon Simple Storage Service (S3) to skalowalna i trwała usługa przechowywania obiektów świadczona przez Amazon Web Services (AWS). Została zaprojektowana do przechowywania i pobierania dowolnej ilości danych z dowolnego miejsca w sieci. S3 jest powszechnie używany w szerokim zakresie przypadków użycia, w tym do tworzenia kopii zapasowych i przywracania, archiwizacji danych, przechowywania i dystrybucji treści, hostingu aplikacji i analizy dużych zbiorów danych.

24. AWS S3 Glacier to niedroga usługa archiwizacyjnego przechowywania danych świadczona przez Amazon Web Services (AWS). Jest ona przeznaczona do długoterminowego przechowywania i archiwizowania danych, które są rzadko dostępne, ale wymagają trwałości i bezpieczeństwa. S3 Glacier oferuje bezpieczną, trwałą i skalowalną pamięć masową do archiwizacji danych przy znacznie niższych kosztach w porównaniu z innymi opcjami pamięci masowej.

25. AWS GuardDuty to usługa wykrywania zagrożeń świadczona przez Amazon Web Services (AWS). Pomaga ona chronić konta i obciążenia AWS poprzez ciągłe monitorowanie złośliwej aktywności i nieautoryzowanych zachowań. GuardDuty wykorzystuje uczenie maszynowe, wykrywanie anomalii i zintegrowaną analizę zagrożeń do identyfikowania potencjalnych zagrożeń bezpieczeństwa i generowania alertów, które można wykorzystać.

26. AWS Key Management Service (KMS): AWS KMS to zarządzana usługa, która pomaga tworzyć i kontrolować klucze szyfrowania używane do szyfrowania danych. Zapewnia bezpieczne i skalowalne rozwiązanie do zarządzania kluczami szyfrowania dla różnych usług AWS i własnych aplikacji. Dzięki KMS można tworzyć, obracać i zarządzać kluczami szyfrowania, a także integrować funkcje szyfrowania z aplikacjami.

27. Amazon Inspector: Amazon Inspector to zautomatyzowana usługa oceny bezpieczeństwa, która pomaga zidentyfikować luki w zabezpieczeniach i naruszenia zgodności w zasobach AWS. Ocenia stan bezpieczeństwa instancji EC2, identyfikuje potencjalne kwestie bezpieczeństwa i dostarcza szczegółowych ustaleń i zaleceń dotyczących środków zaradczych. Inspector pomaga w utrzymaniu bezpiecznego i zgodnego z przepisami środowiska poprzez skanowanie w poszukiwaniu typowych luk w zabezpieczeniach i najlepszych praktyk.

28. AWS Config: AWS Config to usługa umożliwiająca ocenę, audyt i ewaluację konfiguracji zasobów AWS. Zapewnia szczegółowy widok historii konfiguracji zasobów i pomaga ocenić ogólną zgodność i stan bezpieczeństwa środowiska. AWS Config śledzi zmiany w konfiguracji zasobów i umożliwia ustawienie reguł zapewniających zgodność z pożądanymi konfiguracjami.

29. Zarządzanie tożsamością i dostępem AWS (IAM): IAM to kompleksowa usługa zarządzania tożsamością i dostępem, która umożliwia zarządzanie tożsamościami użytkowników i ich dostępem do zasobów AWS. IAM zapewnia precyzyjną kontrolę nad uprawnieniami użytkowników, umożliwiając zarządzanie tym, kto może uzyskać dostęp do zasobów AWS i wykonywać na nich działania. Pomaga egzekwować zasady bezpieczeństwa, tworzyć konta użytkowników i zarządzać nimi oraz integrować się z innymi usługami AWS w celu bezpiecznego uwierzytelniania i autoryzacji.

30. AWS Security Hub: Security Hub to scentralizowana usługa zarządzania bezpieczeństwem, która zapewnia kompleksowy wgląd w stan bezpieczeństwa na wielu kontach AWS. Agreguje i nadaje priorytety ustaleniom dotyczącym bezpieczeństwa z różnych usług AWS, w tym GuardDuty, Inspector i Macie, a także narzędzi bezpieczeństwa innych firm. Security Hub zapewnia pulpit nawigacyjny z praktycznymi spostrzeżeniami i zaleceniami, które pomagają w zarządzaniu i korygowaniu zagrożeń bezpieczeństwa.

31. AWS Network Firewall: Network Firewall to zarządzana usługa zapory sieciowej, która zapewnia ochronę zasobów Amazon VPC (Virtual Private Cloud) na poziomie sieci. Umożliwia ona definiowanie i wymuszanie szczegółowych reguł zapory w celu filtrowania ruchu sieciowego na podstawie adresów IP, protokołów i portów. Network Firewall pomaga chronić VPC przed nieautoryzowanym dostępem i złośliwymi działaniami poprzez sprawdzanie i kontrolowanie ruchu przychodzącego i wychodzącego.

32. AWS Secrets Manager: Secrets Manager to usługa, która pomaga bezpiecznie przechowywać i zarządzać sekretami, takimi jak klucze API, poświadczenia bazy danych i hasła. Eliminuje ona potrzebę kodowania poufnych informacji w aplikacjach, zapewniając centralne repozy-

torium do przechowywania sekretów. Secrets Manager integruje się z innymi usługami AWS i obsługuje automatyczną rotację sekretów w celu zwiększenia bezpieczeństwa i zgodności.

33. Amazon Macie: Macie to w pełni zarządzana usługa bezpieczeństwa i prywatności danych, która wykorzystuje uczenie maszynowe do automatycznego wykrywania, klasyfikowania i ochrony wrażliwych danych przechowywanych w Amazon S3. Pomaga zidentyfikować wrażliwe dane, takie jak dane osobowe (PII), własność intelektualna i dane finansowe, a także zapewnia alerty i zalecenia dotyczące zabezpieczania i monitorowania wrażliwych zasobów danych.

34. Amazon CloudWatch: CloudWatch to usługa monitorowania i obserwowalności, która zapewnia wgląd w zasoby i aplikacje AWS. Gromadzi i śledzi metryki, dzienniki i zdarzenia, umożliwiając monitorowanie wydajności i kondycji infrastruktury. CloudWatch umożliwia ustawianie alarmów, tworzenie niestandardowych pulpitów nawigacyjnych i uzyskiwanie wglądu w wykorzystanie zasobów, wydajność aplikacji i kwestie operacyjne.

35. AWS X-Ray: X-Ray to rozproszona usługa śledzenia, która pomaga analizować i debugować aplikacje w architekturze mikrousług. Umożliwia śledzenie żądań podczas ich przechodzenia przez aplikacje, zapewniając wgląd w działanie usług oraz identyfikację wąskich gardeł i błędów. X-Ray pomaga zrozumieć kompleksowe zachowanie aplikacji oraz poprawić ich wydajność i niezawodność.

36. AWS CloudTrail: CloudTrail to usługa zapewniająca kompleksowe funkcje audytu i rejestrowania dla konta AWS. Rejestruje całą aktywność API i zdarzenia w zasobach AWS, umożliwiając śledzenie zmian, badanie incydentów bezpieczeństwa i spełnianie wymogów zgodności. Dzienniki CloudTrail mogą być wykorzystywane do analizy bezpieczeństwa, rozwiązywania problemów i celów zarządzania.

37. Usługa Amazon Elasticsearch: Elasticsearch to w pełni zarządzana usługa wyszukiwania i usługa analityczna oparta na otwartym silniku Elasticsearch. Jest to zapewnia skalowalną i niezawodną platformę do przechowywania, wyszukiwania i analizowania dużych ilości ustrukturyzowanych i nieustrukturyzowanych danych. Elasticsearch jest powszechnie

używany do analizy dzienników, wyszukiwania pełnotekstowego, analizy w czasie rzeczywistym i tworzenia pulpitów nawigacyjnych do eksploracji danych.

38. AWS Systems Manager: Systems Manager to zestaw narzędzi do zarządzania i automatyzacji zadań operacyjnych na zasobach AWS. Zapewnia scentralizowany interfejs do przeglądania i kontrolowania infrastruktury, zarządzania poprawkami i inwentaryzacją oprogramowania, automatyzacji zarządzania konfiguracją oraz bezpiecznego przechowywania i dystrybucji sekretów. Systems Manager pomaga utrzymać higienę operacyjną, usprawnić zarządzanie zasobami i uprościć zadania administracyjne.

39. AWS CloudFormation: CloudFormation to usługa, która umożliwia definiowanie i udostępnianie infrastruktury AWS jako kodu. Pozwala ona na opisanie zasobów za pomocą deklaratywnego szablonu, który może być kontrolowany wersjami i wdrażany spójnie w wielu środowiskach. CloudFormation automatyzuje tworzenie, aktualizowanie i usuwanie zasobów, ułatwiając zarządzanie i skalowanie infrastruktury.

40. Amazon Simple Queue Service (SQS): SQS to w pełni zarządzana usługa kolejkowania wiadomości, która umożliwia oddzielenie i asynchroniczną komunikację między rozproszonymi komponentami aplikacji. Umożliwia wysyłanie, przechowywanie i odbieranie wiadomości między komponentami oprogramowania, pomagając w tworzeniu skalowalnych i odpornych na błędy systemów. SQS zapewnia niezawodne dostarczanie wiadomości i obsługuje zarówno kolejki standardowe, jak i FIFO (First-In-First-Out).

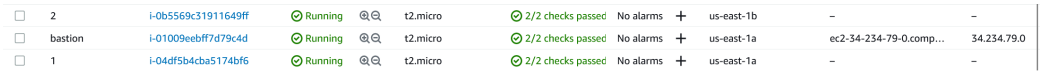
41. Amazon Simple Notification Service (SNS): SNS to elastyczna i w pełni zarządzana usługa przesyłania wiadomości, która umożliwia wysyłanie i odbieranie powiadomień z aplikacji i usług. Obsługuje różne protokoły przesyłania wiadomości, w tym e-mail, SMS, mobilne powiadomienia push i punkty końcowe HTTP/S. SNS umożliwia nadawanie wiadomości do wielu odbiorców, upraszcza architekturę aplikacji i integruje się z innymi usługami AWS.

42. Amazon EventBridge: EventBridge to bezserwerowa usługa magistrali zdarzeń, która umożliwia tworzenie architektur opartych na zdarze-

niach i łatwą integrację różnych aplikacji i usług. Umożliwia ona kierowanie zdarzeń z różnych źródeł do docelowych miejsc przetwarzania lub wyzwalania akcji. EventBridge upraszcza przepływy pracy sterowane zdarzeniami i umożliwia luźne łączenie komponentów w aplikacjach.

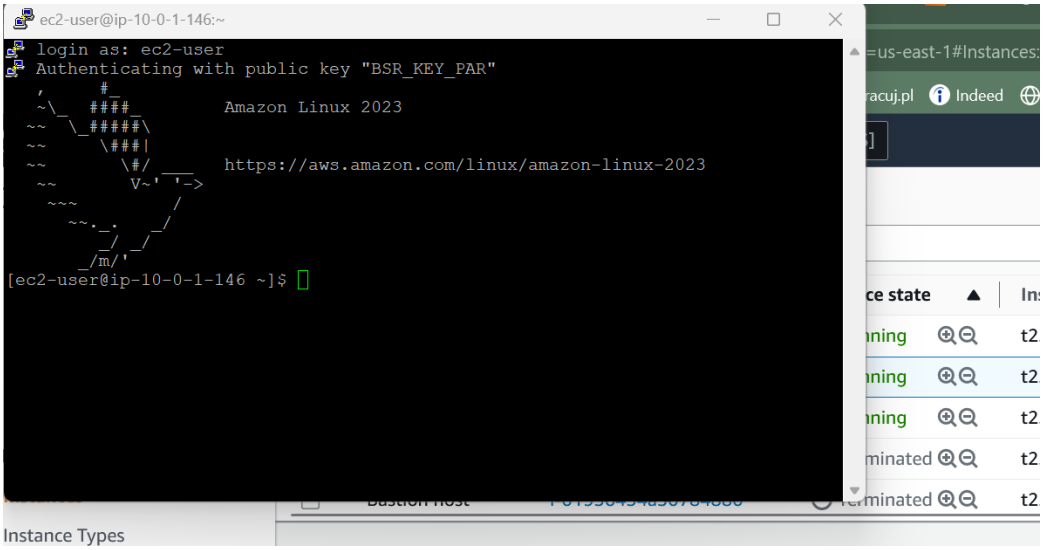
7 Realizacja projektu w AWS

7.1 Tworzenie EC2

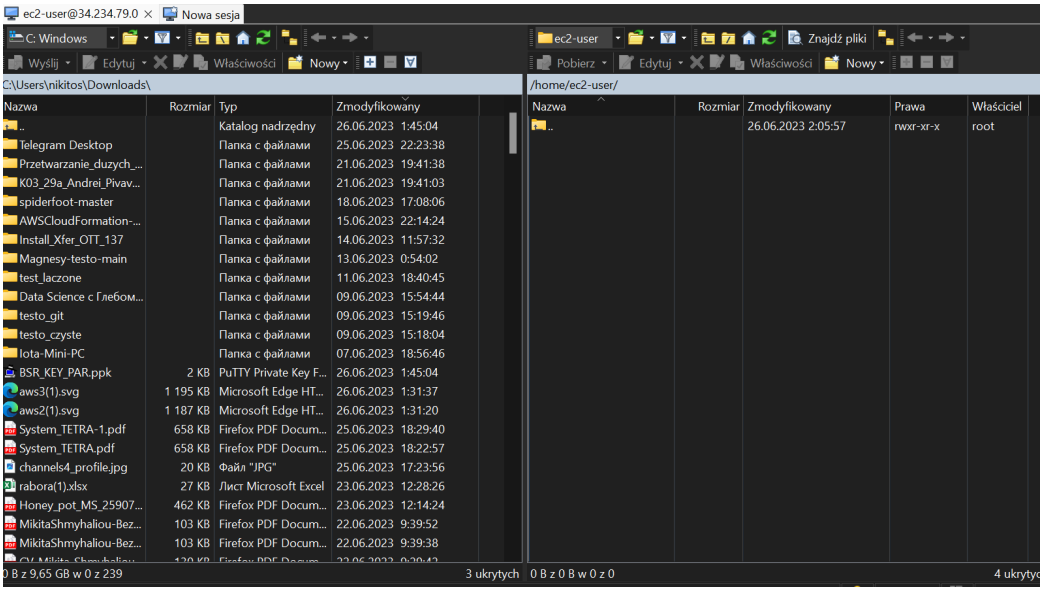


Rysunek 3: Tworzenie EC2

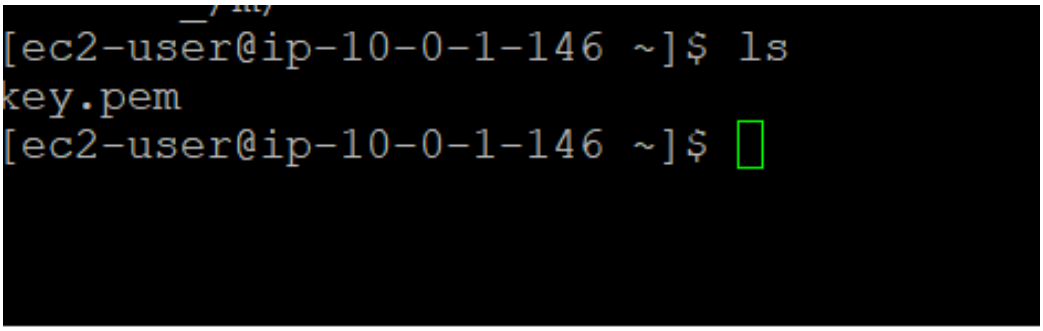
7.2 Bastion Host



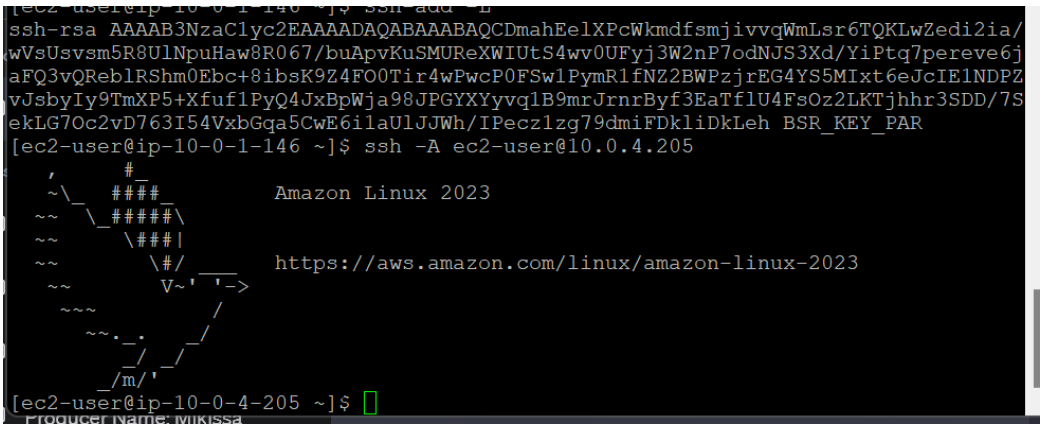
Rysunek 4: Logowanie na Bastion



Rysunek 5: Wysyłanie private key

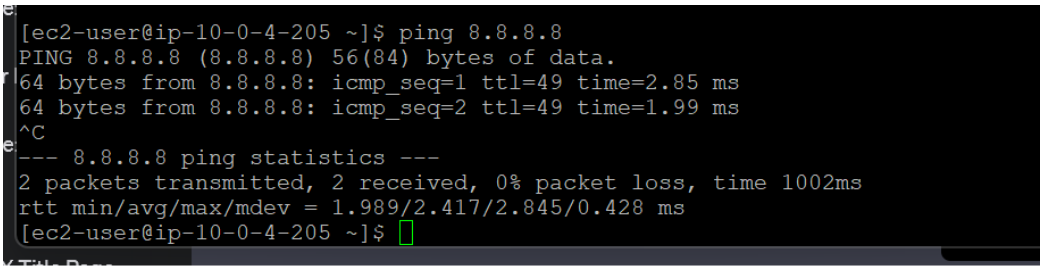


Rysunek 6: Demonstracja private key

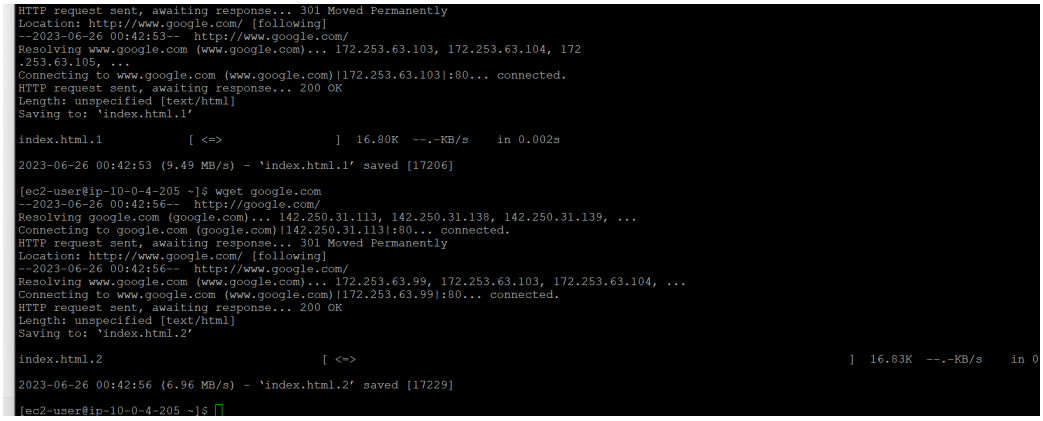


Rysunek 7: Logowanie do private subnet EC2

7.2.1 Nat Gateway

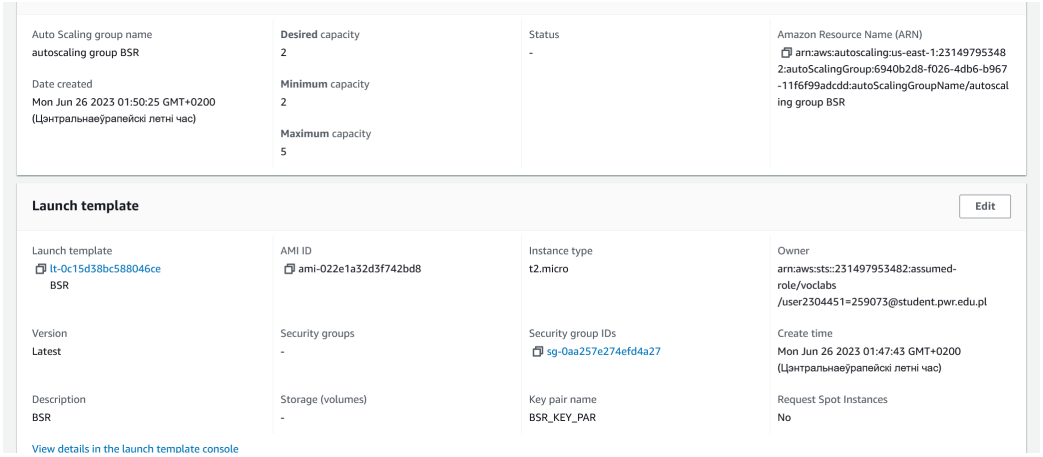


Rysunek 8: Działanie Nat Gateway



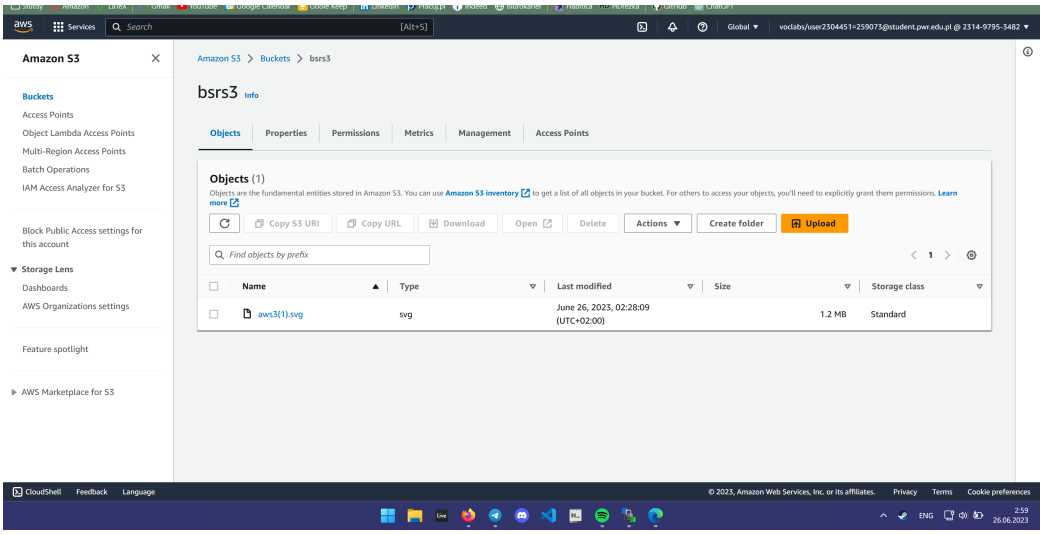
Rysunek 9: Działanie Nat Gateway

7.3 ASG

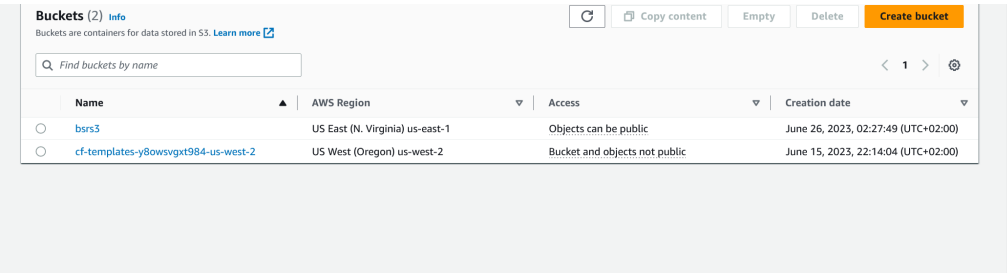


Rysunek 10: Configuracja ASG

7.4 S3



Rysunek 11: Ojekt w S3



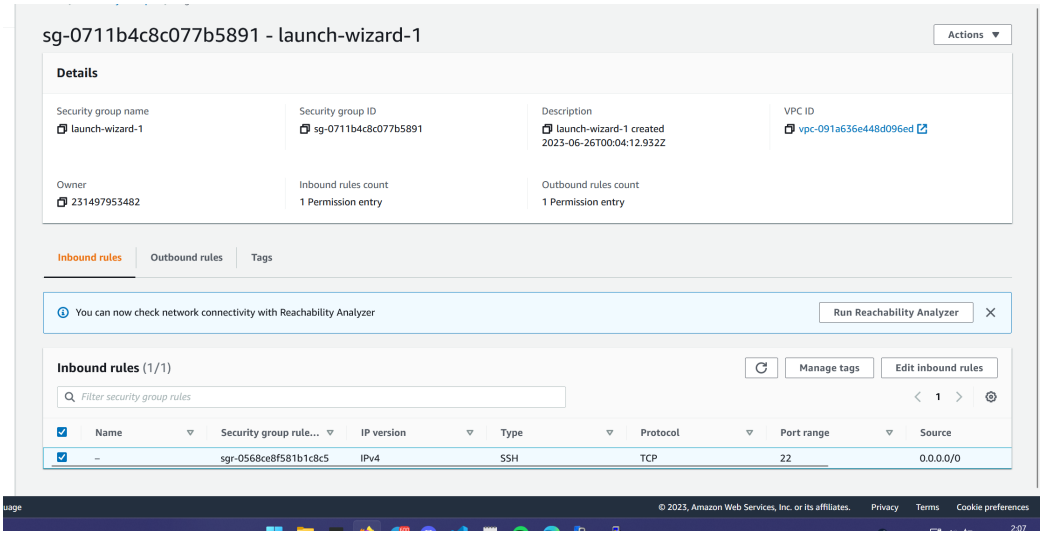
Rysunek 12: Wiaderki

```
[ec2-user@ip-10-0-4-205 ~]$ aws s3 ls
2023-06-26 00:27:49 bsrs3
2023-06-15 20:14:04 cf-templates-y8owsvgxt984-us-west-2
[ec2-user@ip-10-0-4-205 ~]$ ls
```

Rysunek 13: Działanie S3

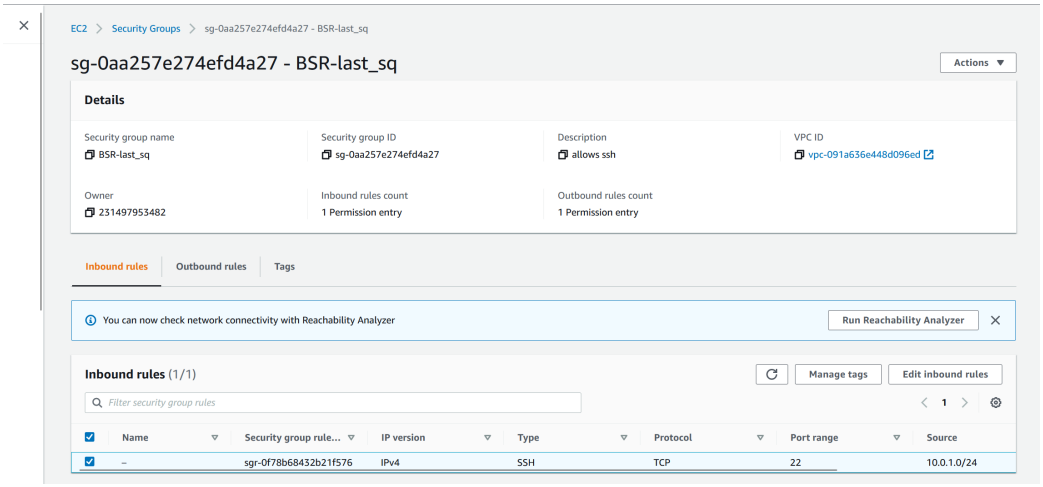
7.5 Security groups

7.5.1 Dla Bastion Host



Rysunek 14: Security groups dla Bastiona

7.5.2 Dla EC2



Rysunek 15: Security groups dla EC2

8 Bezpieczeństwo

Aby zapewnić bezpieczeństwo danych przechowywanych w chmurze, banki muszą wdrożyć szereg środków bezpieczeństwa, takich jak:

1. Kontrola dostępu
2. Szyfrowanie
3. Firewall
4. Bezpieczeństwo sieci
5. Audyt i monitoring
6. Regularnie aktualizować systemy

Oprócz środków technicznych, banki muszą również spełniać obowiązujące wymogi regulacyjne związane z ochroną danych, prywatnością danych i regulacjami finansowymi. Banki muszą również zapewnić, że ich dostawcy usług w chmurze spełniają te wymogi oraz że istnieją odpowiednie umowy, które chronią interesy banku. Kluczowe standardy i normy:

1. ISO/IEC 27001: Jest to międzynarodowy standard dla systemów zarządzania bezpieczeństwem informacji (ISMS), który zapewnia ramy dla wdrażania i zarządzania kontrolami bezpieczeństwa informacji. Obejmuje ona szereg kontroli, które można wykorzystać do ochrony danych przechowywanych w chmurze, takich jak kontrola dostępu, szyfrowanie i odzyskiwanie danych po awarii.
2. PCI DSS: Payment Card Industry Data Security Standard (PCI DSS) to zestaw standardów bezpieczeństwa ustanowionych przez głównych operatorów kart kredytowych w celu zapewnienia ochrony danych posiadaczy kart. Zawiera on wymagania związane z przechowywaniem i przetwarzaniem danych posiadaczy kart w chmurze.
3. NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework to ramy zarządzania ryzykiem cybernetycznym, które zapewniają zestaw najlepszych praktyk w zakresie zabezpieczania danych przechowywanych w chmurze.

4. Europejski Urząd Nadzoru Bankowego (EBA) wydał wytyczne dotyczące outsourcingu czynności bankowych, w tym cloud computingu. Wytyczne te stanowią ramy dla banków w zakresie oceny ryzyka związanego z przetwarzaniem w chmurze oraz wdrażania odpowiednich środków bezpieczeństwa w celu ochrony danych wrażliwych.

5. RODO to kolejna regulacja, która dotyczy branży bankowej. RODO określa zasady ochrony danych osobowych i ma zastosowanie do wszystkich organizacji, które przetwarzają dane osobowe obywateli UE, niezależnie od tego, gdzie organizacja ma siedzibę. Rozporządzenie zawiera wymagania dotyczące ochrony danych w fazie projektowania i domyślnej, a także wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa.

Oprócz tych standardów i norm istnieją również różne certyfikaty i audyty, którym banki mogą się poddać, aby wykazać zgodność z wymogami bezpieczeństwa. Na przykład:

1. SOC 2 (Service Organization Control 2) to standard audytu, który ocenia kontrole organizacji usługowej związane z bezpieczeństwem, dostępnością, integralnością przetwarzania, poufnością i prywatnością.

2. Cloud Security Alliance (CSA) zapewnia zestaw wytycznych dotyczących bezpiecznego korzystania z chmury obliczeniowej.

3. CSA Security, Trust, and Assurance Registry (STAR), który jest programem certyfikacji dla dostawców usług w chmurze.