Raport projekt 2

Zaawansowane rozwiązania chmurowe

19.01.2026

Dominika Kołowrotkiewicz

Spis treści

1 Repozytorum

Cały kod dostępny jest w repozytorium na githubie: ArtGallery na gałęzi "projekt_2".

2 Informacje ogólne

Wszystkie serwisy zostału uruchomione na instancjeach EC2. Dla każdej instancji utworzono własną security group. Każda instancja EC2 używa profilu z rolą Lab oraz korzysta z ami spełniającego poniższe kryteria:

- jest opublikowane przez AWS,
- jest najnowszą wersją spełniającą pozostałe filtry,
- według filtru nazwy jest linuxem z 2023 roku,
- ma architekturę Intel / AMD (x86_64)
- ma typ wirtualizacji hvm.

3 Keycloak

3.1 Security group

Security group otwiera porty 8180 (główny port keycloak) i 9000 (management/health) dla zasobów w security group alb, czyli w praktyce tylko zasoby przypisane do security group load balancera mogą połączyć się z Keycloak.

3.2 Target group

Target Group definiuje sposób kierowania ruchu z Application Load Balancer do instancji EC2 z uruchomionym serwisem Keycloak. Ruch aplikacyjny jest przekazywany na port 8180 z wykorzystaniem protokołu HTTP, natomiast stan zdrowia instancji weryfikowany jest niezależnie poprzez dedykowany endpoint /health/ready na porcie 9000.

Zasób aws_lb_target_group_attachment rejestruje instancję EC2 z uruchomionym serwisem Keycloak w grupie docelowej Application Load Balancer. Dzięki temu instancja zaczyna podlegać mechanizmom health check oraz otrzymywać ruch przekazywany przez load balancer na porcie 8180.

3.3 Listener rule

Reguła listenera Application Load Balancer realizuje routing oparty o ścieżkę URL, przekierowując żądania związane z serwisem Keycloak do dedykowanej grupy docelowej. Wykorzystane wzorce ścieżek obejmują kluczowe endpointy protokołów OpenID Connect oraz interfejsu administracyjnego: "/.well-known/*", "/realms/*", "/resources/*", "/admin/*".

3.4 Instancja EC2

Zastosowany typ instancji t3.small jest w pełni kompatybilny z użytym obrazem Amazon Linux 2023, ponieważ oba wykorzystują architekturę x86_64 oraz typ wirtualizacji HVM.

3.5 Skrypt user-data

Skrypt user-data-keycloak.sh.tpl jest wykonywany automatycznie podczas pierwszego uruchomienia instancji EC2 i odpowiada za instalację, konfigurację oraz uruchomienie serwisu Keycloak.
Kroki wykonywane w skrypcie:

- Definicja zmiennych konfiguracyjnych
- Instalacja zależności systemowych
- Utworzenie użytkownika systemowego
- Pobranie i instalacja Keycloak
- Utworzenie usługi systemd z parametrami uruchomienia Keycloak
- Uruchomienie usługi
- Oczekiwanie na gotowość aplikacji
- Logowanie do Keycloak CLI (kcadm)
- Utworzenie domeny (realm)
- Utworzenie klienta (dla frontendu)

4 Postgres

4.1 Generowanie hasła

Wykorzystano AWS Secrets Manager do bezpiecznego przechowywania sekretów dla bazy danych. Hasło generowane jest automatycznie jako losowy ciąg znaków spełniający wymagania złożoności i zapisywane w sekrecie w formacie JSON wraz z nazwą użytkownika.

4.2 Security group

Security group otwiera port 5432 dla zasobów w security group backendu.

4.3 Instancja EC2

Zastosowany typ instancji t3.small jest w pełni kompatybilny z użytym obrazem Amazon Linux 2023, ponieważ oba wykorzystują architekturę x86_64 oraz typ wirtualizacji HVM.

4.4 EBS

Stworzono zaszyfrowany wolumen EBS typu gp3 przeznaczony na dane bazy PostgreSQL i dołączono go do instancji EC2. Zastosowanie typu gp3 zapewnia stabilną wydajność przy niższych kosztach w porównaniu do starszych typów wolumenów. Oddzielenie dysku danych od dysku systemowego zwiększa bezpieczeństwo oraz ułatwia zarządzanie i odzyskiwanie danych.

4.5 Skrypt user-data

Skrypt user-data-postgres.sh.tpl jest wykonywany automatycznie podczas pierwszego uruchomienia instancji EC2 i odpowiada za instalację, konfigurację oraz uruchomienie PostgreSQL.
Kroki wykonywane w skrypcie:

- Instalacja zależności systemowych
- Wykrycie i montowanie dodatkowego wolumenu EBS
- Przygotowanie katalogu danych PostgreSQL
- Nadpisanie konfiguracji systemd (PGDATA)
- Inicjalizacja bazy danych
- Konfiguracja dostępu sieciowego
- Uruchomienie i włączenie PostgreSQL
- Utworzenie użytkownika bazy danych
- Utworzenie bazy danych

5 MinIO

5.1 Generowanie kluczy

Wykorzystano AWS Secrets Manager do bezpiecznego przechowywania sekretów dla MinIO. Klucz sekretu generowany jest automatycznie jako losowy ciąg znaków spełniający wymagania złożoności i zapisywane w sekrecie w formacie JSON wraz z kluczem dostępu.

5.2 Security group

Security group otwiera port 9000 dla zasobów w security group alb.

5.3 Target group

Target Group definiuje sposób kierowania ruchu z Application Load Balancer do instancji EC2 z uruchomionym serwisem MinIO. Ruch aplikacyjny jest przekazywany na port 9000 z wykorzystaniem protokołu HTTP, natomiast stan zdrowia instancji weryfikowany jest niezależnie poprzez dedykowany endpoint /minio/health/live na porcie 9000.

Zasób aws_lb_target_group_attachment rejestruje instancję EC2 z uruchomionym serwisem MinIO w grupie docelowej Application Load Balancer. Dzięki temu instancja zaczyna podlegać mechanizmom health check oraz otrzymywać ruch przekazywany przez load balancer na porcie 9000.

5.4 Listener rule

Reguła listenera Application Load Balancer realizuje routing oparty o ścieżkę URL, przekierowując żądania związane z serwisem MinIO do dedykowanej grupy docelowej. Wykorzystane wzorce ścieżek obejmują endpointy: "/bucket/*".

5.5 Instancja EC2

Zastosowany typ instancji t3.small jest w pełni kompatybilny z użytym obrazem Amazon Linux 2023, ponieważ oba wykorzystują architekturę x86_64 oraz typ wirtualizacji HVM.

5.6 EBS

Stworzono zaszyfrowany wolumen EBS typu gp3 przeznaczony na zdjęcia i dołączono go do instancji EC2.

5.7 Skrypt user-data

Skrypt user-data-minio.sh.tpl jest wykonywany automatycznie podczas pierwszego uruchomienia instancji EC2 i odpowiada za instalację, konfigurację oraz uruchomienie MinIO.
Kroki wykonywane w skrypcie:

- Instalacja zależności systemowych
- Wykrycie i montowanie dodatkowego wolumenu EBS
- Pobranie i instalacja MinIO
- Uzupełnienie zmiennych środowiskowych dla MinIO
- Konfigurowacja serwisu MinIO
- Uruchomienie serwisu
- Ustawienie aliasu
- Utworzenie bucketu i przyznanie dostępu

6 Prometheus

6.1 Security group

Security group otwiera port 9090 dla zasobów w security group alb.

6.2 Target group

Target Group definiuje sposób kierowania ruchu z Application Load Balancer do instancji EC2 z uruchomionym serwisem Prometheus. Ruch aplikacyjny jest przekazywany na port 9090 z wykorzystaniem protokołu HTTP, natomiast stan zdrowia instancji weryfikowany jest niezależnie poprzez dedykowany endpoint /prometheus/-/healthy na porcie 9000.

Zasób aws_lb_target_group_attachment rejestruje instancję EC2 z uruchomionym serwisem Prometheus w grupie docelowej Application Load Balancer. Dzięki temu instancja zaczyna podlegać mechanizmom health check oraz otrzymywać ruch przekazywany przez load balancer na porcie 9090.

6.3 Listener rule

Reguła listenera Application Load Balancer realizuje routing oparty o ścieżkę URL, przekierowując żądania związane z serwisem Prometheus do dedykowanej grupy docelowej. Wykorzystane wzorce ścieżek obejmują endpointy: "/prometheus/*".

6.4 Instancja EC2

Zastosowany typ instancji t3.small jest w pełni kompatybilny z użytym obrazem Amazon Linux 2023, ponieważ oba wykorzystują architekturę x86_64 oraz typ wirtualizacji HVM.

6.5 Skrypt user-data

Skrypt user-data-prometheus.sh.tpl jest wykonywany automatycznie podczas pierwszego uruchomienia instancji EC2 i odpowiada za instalację, konfigurację oraz uruchomienie Prometheus.
Kroki wykonywane w skrypcie:

- Instalacja zależności systemowych
- Utworzenie katalogów
- Pobranie i instalacja Prometheus
- Utworzenie konfiguracji
- Utworzenie serwisu
- Uruchomienie serwisu

7 Grafana

7.1 Security group

Security group otwiera port 3000 dla zasobów w security group alb.

7.2 Target group

Target Group definiuje sposób kierowania ruchu z Application Load Balancer do instancji EC2 z uruchomionym serwisem Grafana. Ruch aplikacyjny jest przekazywany na port 3000 z wykorzystaniem protokołu HTTP, natomiast stan zdrowia instancji weryfikowany jest niezależnie poprzez dedykowany endpoint /api/health na porcie 3000.

Zasób aws_lb_target_group_attachment rejestruje instancję EC2 z uruchomionym serwisem Grafana w grupie docelowej Application Load Balancer. Dzięki temu instancja zaczyna podlegać mechanizmom health check oraz otrzymywać ruch przekazywany przez load balancer na porcie 3000.

7.3 Listener rule

Reguła listenera Application Load Balancer realizuje routing oparty o ścieżkę URL, przekierowując żądania związane z serwisem Prometheus do dedykowanej grupy docelowej. Wykorzystane wzorce ścieżek obejmują endpointy: "/grafana/*".

7.4 Instancja EC2

Zastosowany typ instancji t3.small jest w pełni kompatybilny z użytym obrazem Amazon Linux 2023, ponieważ oba wykorzystują architekturę x86_64 oraz typ wirtualizacji HVM.

7.5 Skrypt user-data

Skrypt user-data-grafana.sh.tpl jest wykonywany automatycznie podczas pierwszego uruchomienia instancji EC2 i odpowiada za instalację, konfigurację oraz uruchomienie Grafana.
Kroki wykonywane w skrypcie:

- Konfiguracja repozytorium Grafana OSS
- Przygotowanie katalogów provisioningowych

- Konfiguracja źródła danych Prometheus
- Konfiguracja dostawcy dashboardów
- Provisioning dashboardu aplikacyjnego
- Instalacja Grafany
- Konfiguracja serwera Grafana
- Uruchomienie usługi Grafana