

Projekt 1.

Instrukcja do wdrożenia aplikacji

1. Na Cloud9 opartym na Ubuntu instalujemy terraforma i ansible.

```
sudo snap install terraform --classic
```

```
pip install --user ansible
```

Dla potwierdzenia instalacji możemy uruchomić poniższe komendy:

```
terraform -version
```

```
ansible -version
```

2. Klonujemy repozytorium.

<https://github.com/astypczy/ZRCwAW.git>

3. Wchodzimy do folderu terraform i uruchamiamy kolejno komendy:

```
terraform init; terraform plan; terraform apply;
```

4. Czekamy na zakończenie działania procesu.

5. Używając ssh łączymy się z dwiema instancjami.

```
ssh -i <KEY_PAIR> ubuntu@<EC2_PUBLIC_IP>
```

6. Na maszynie Backend uruchamiamy aplikację używając:

```
java -jar /opt/ZRCwAW/ec2/backend/target/project-0.0.1-SNAPSHOT.jar
```

7. Na maszynie Frontend uruchamiamy aplikację poprzez komendy:

```
cd /opt/ZRCwAW/ec2/frontend
```

```
sudo ng serve --host 0.0.0.0 --port 4200
```

8. Czekamy na zbudowanie aplikacji.

9. Po zbudowaniu możemy wejść na stronę: <http://52.20.47.142:4200>.

10. Można korzystać z aplikacji.

Tworzenie Cognito

Step 2

[Configure security requirements](#)

Step 3

Configure sign-up experience

Step 4

Configure message delivery

Step 5

Integrate your app

Step 6

Review and create

Authentication providers

Configure the providers that are available to users when they sign in.

Provider types

Choose whether users will sign in to your Cognito user pool, a federated identity provider, or both. Amazon Cognito has different pricing for federated users and user pool users. [Learn more about pricing](#)

☒ **Cognito user pool**

Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

☐ **Federated identity providers**


Users can sign in using credentials from social identity providers like Facebook, Google, Amazon, and Apple; or using credentials from external directories through SAML or Open ID Connect. You can manage user attribute mappings and security for federated users in your user pool.

Cognito user pool sign-in options

[Info](#)

Choose the attributes in your user pool that are used to sign in. If you select only one attribute, or you select a user name and at least one other attribute, your user can sign in with all of the selected options. If you select only phone number and email, your user will be prompted to select one of the two sign-in options when they sign up.

☐ User name
☒ Email
☐ Phone number

 Cognito user pool sign-in options can't be changed after the user pool has been created.

Cancel

Next

Password policy [Info](#)

Create a password policy to define the length and complexity of the passwords your users can set.

Password policy mode [Info](#)



Cognito defaults

Use default password requirements.



Custom

Use password requirements that you define.

Password minimum length

8 character(s)

Password requirements

Contains at least 1 number

Contains at least 1 special character

Contains at least 1 uppercase letter

Contains at least 1 lowercase letter

MFA enforcement [Info](#)

☐ **Require MFA - Recommended**

Users must provide an additional authentication factor when signing in.

☐ **Optional MFA**

Users can sign in with a single authentication factor, and can choose to add additional authentication factors.

☒ **No MFA**

Users can only sign in with a single authentication factor. This is the least secure option.

User account recovery

Configure how users will recover their account when they forget their password. Recipient message and data rates apply.

Self-service account recovery [Info](#)

☒ **Enable self-service account recovery - Recommended**

Allow forgot-password operations in your user pool. In the hosted UI sign-in page, a "Forgot your password?" link is displayed. When this feature is not enabled, administrators reset passwords with the Cognito API.

Delivery method for user account recovery messages [Info](#)

Select how your user pool will deliver messages when users request an account recovery code. SMS messages are charged separately by Amazon SNS. Email messages are charged separately by Amazon SES. [Learn more about pricing.](#)

☒ **Email only**

☐ SMS only

☐ Email if available, otherwise SMS

☐ SMS if available, otherwise email

☐ SMS if available, otherwise email, and allow a user to reset their password via SMS if they are also using it for MFA

Cancel

Previous

Next

Configure sign-up experience [Info](#)

Determine how new users will verify their identities when signing up and which attributes should be required or optional during the user sign-up flow.

Self-service sign-up [Info](#)

Choose whether new users of your app can register for an account themselves.

Self-registration [Info](#)

☒ **Enable self-registration**

Display a "Sign up" link on the sign-in page in the hosted UI, and allow the use of public APIs to create new user accounts. When this feature is not enabled, federation and administrative API operations create user profiles.

i If you activate user sign-up in your user pool, anyone on the internet can sign up for an account and sign in to your apps. Don't enable self-registration in your user pool until you want to open your app to public sign-up. [Learn more](#)

Cognito-assisted verification and confirmation [Info](#)

Automatically send

☒ **Allow Cognito to automatically send messages to verify and confirm - Recommended**

Amazon Cognito sends a verification message with a code that the user must enter. For new users, this will verify the attribute and confirm their account.

☐ **Don't automatically send messages**

Amazon Cognito doesn't send messages to users who add or change an attribute. Update attributes and confirm users with administrative API operations or Lambda triggers.

Attributes to verify [Info](#)

Choose the user contact attribute that Cognito will send a verification message to. Recipient message and data rates apply when you use SMS.

☐ **Send SMS message, verify phone number**

Verify with SMS to allow users to use their phone number for sign-in, MFA, and account recovery. SMS messages are charged separately by Amazon SNS.

☒ **Send email message, verify email address**

Verify with email to allow users to use their email address for sign-in, MFA, and account recovery. Email messages are charged separately by Amazon SES.

☐ **Send SMS message if phone number is available, otherwise send email message**

You must build custom code when you want to verify both email and phone numbers at user account creation.

Verifying attribute changes [Info](#)

☒ **Keep original attribute value active when an update is pending - Recommended**

Active attribute values when an update is pending [Info](#)

Choose the attributes that you want to keep active when an update to their value is pending. Your users can receive messages and sign in with the original attribute value until they verify the new value.

☐ Phone number

☒ Email address

☐ Phone number and email address

Required attributes [Info](#)

Choose the attributes that are required when a new user is created. Cognito assigns all users a set of standard attributes based on the OpenID Connect (OIDC) standard.

Required attributes based on previous selections

-

Additional required attributes

Select attributes

given_name X

family_name X

email X



Required attributes can't be changed once this user pool has been created.

dodatkowo dodajemy

Custom isSeller: String

Email

Configure how your user pool sends email messages to users.

Email provider [Info](#)

☐ Send email with Amazon SES - Recommended
Send email messages using an Amazon SES verified identity in your account. Recommended for higher email volume and production workloads. Required for email MFA.

☒ Send email with Cognito
Use Cognito's default email address as a temporary start for development. You can use it to send up to 50 emails a day.

You must have configured a verified sender with [Amazon SES](#) to use the SES feature. [Learn more](#)

SES Region [Info](#)
US East (N. Virginia)

FROM email address [Info](#)
By default "no-reply@verificationemail.com" will be used. You can also choose a different email address that you have previously verified with Amazon SES.

no-reply@verificationemail.com

REPLY-TO email address - optional [Info](#)
If you set an invalid reply-to address, sending restrictions may be imposed on your account.

Enter an email address

Cancel

Previous

Next

Integrate your app [Info](#)

Set up app integration for your user pool with Cognito's built-in authentication and authorization flows.

User pool name

Create a friendly name for your user pool.

User pool name

cognitospringboot

User pool names are limited to 128 characters or less. Names may only contain alphanumeric characters, spaces, and the following special characters: + = , . @ -

Your user pool name can't be changed once this user pool is created.

Nie używamy hosted ui

Wybieramy Public client, Don't generate a client secret, reszta opcji domyślnie

Cognito zostało skonfigurowane.

Tworzenie RDS


W zakładce RDS tworzymy instancję.


☒ **Standard create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.


☐ **Easy create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.


Engine options


Engine type [Info](#)


☐ Aurora (MySQL Compatible)



☐ MySQL



☐ MariaDB


☐ Microsoft SQL Server


☐ Aurora (PostgreSQL Compatible)


☒ PostgreSQL


☐ Oracle


☐ IBM Db2


Engine version [Info](#)

View the engine versions that support the following database features.

▼ Hide filters

☐ Show only versions that support the Multi-AZ DB cluster [Info](#)
Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Engine version

PostgreSQL 16.3-R3

Templates

Choose a sample template to meet your use case.

☐ **Production**
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
This instance is intended for development use outside of a production environment.

☒ **Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

☒ Multi-AZ DB Cluster
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

☐ Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

☐ Single DB instance (not supported for Multi-AZ DB cluster snapshot)
Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

postgres

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

☐ Managed in AWS Secrets Manager - most secure
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

☒ Self managed
Create your own password or have RDS create a password that you manage.

Resztę opcji zostawiamy domyślnie.

Tworzenie instancji EC2

Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Info


Name

test

Add additional tags







Info


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 [Search our full catalog including 1000s of application and OS images](#)

Recents

Quick Start

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Linux
					


Browse more AMIs
Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0866a3c8686eaeeba (64-bit (x86)) / ami-0325498274077fac5 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture

64-bit (x86)

AMI ID

ami-0866a3c8686eaeeba

Username

ubuntu



Verified provider

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t3.medium

Family: t3 2 vCPU 4 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0979 USD per Hour
On-Demand Windows base pricing: 0.06 USD per Hour
On-Demand Linux base pricing: 0.0416 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0451 USD per Hour
On-Demand RHEL base pricing: 0.0704 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey



[Create new key pair](#)

▼ Network settings [Info](#)

[Edit](#)

Network [Info](#)

vpc-04ad86e4bf7e5da9b

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

[Additional charges apply](#) when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server



Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

