

POLITECHNIKA WROCŁAWSKA

INFORMATYKA STOSOWANA

PROJEKTOWANIE I WDRAŻANIE
SYSTEMÓW W CHMURZE

Projekt 1 - Raport

Prowadzący:

dr inż. Rafał Palak

Autor:

Jonasz Lazar, 263898

Spis treści

1	Dokumentacja REST API	2
2	Konfiguracja Amazon Web Services	4
2.1	AWS Cognito	4
2.2	AWS S3	5
2.3	AWS RDS	7
2.4	AWS Elastic Beanstalk	11
2.5	AWS CloudWatch	16

1 Dokumentacja REST API

Poniżej przedstawiono dokumentację endpointów REST API, wygenerowaną automatycznie przez Swagger UI, która przedstawia strukturę żądań, odpowiedzi oraz wymagane uprawnienia.

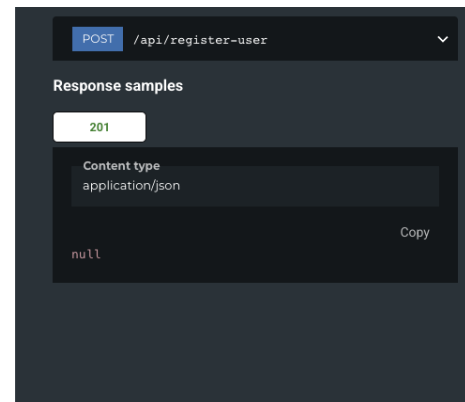
Register a new user

Registers a new user using attributes from the validated JWT token.

AUTHORIZATIONS: > *JWTBearer or JWTBearer*

Responses

> 201 User created successfully
— 204 User already exists
— 400 Missing required user attributes in token
— 401 Unauthorized – invalid or missing token



Rysunek 1: Dokumentacja endpointu POST /api/register-user

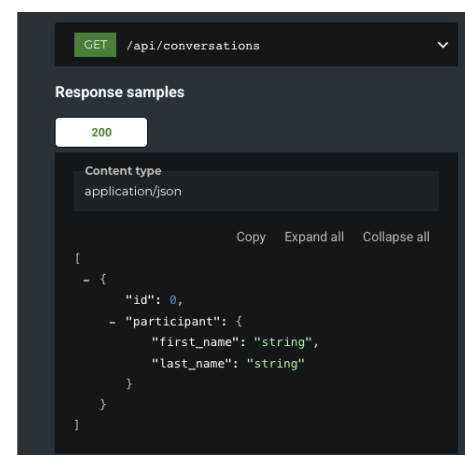
Get user conversations

Returns a list of conversations for the currently authenticated user. Each item includes the conversation ID and participant details.

AUTHORIZATIONS: > *JWTBearer or JWTBearer*

Responses

> 200 List of conversations returned successfully
— 401 Unauthorized – invalid or missing token



Rysunek 2: Dokumentacja endpointu GET /api/conversations

Get messages from a conversation

Retrieves all messages from a given conversation, ordered by time sent. The user must be a participant of the conversation.

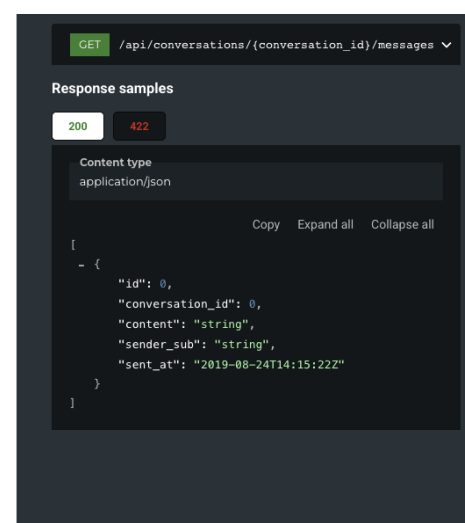
AUTHORIZATIONS: > *JWTBearer or JWTBearer*

PATH PARAMETERS

conversation_id	integer (Conversation Id)
required	

Responses

> 200 List of messages returned successfully
— 401 Unauthorized – invalid or missing token
— 403 User is not authorized to access this conversation
— 404 Conversation not found
> 422 Validation Error



Rysunek 3: Dokumentacja endpointu GET /api/conversations/{conversation_id}/messages

Send a text message

Sends a new text message in a specified conversation. The sender must be a participant of that conversation.

AUTHORIZATIONS: >	JWTBearer or JWTBearer
REQUEST BODY SCHEMA: application/json	
conversation_id required	integer (Conversation Id) ID of the conversation
content required	string (Content) Text content of the message

Responses

> 201	Message sent successfully
— 401	Unauthorized – invalid or missing token
— 403	User is not authorized to send message in this conversation
— 404	Conversation not found
> 422	Validation Error

POST /api/messages

Request samples

Payload

Content type
application/json

Copy

```
{
  "conversation_id": 0,
  "content": "string"
}
```

Response samples

201 422

Content type
application/json

Copy

```
{
  "id": 0,
  "conversation_id": 0,
  "content": "string",
  "sender_sub": "string",
  "sent_at": "2019-08-24T14:15:22Z"
}
```

Rysunek 4: Dokumentacja endpointu POST /api/messages

Send a media message

Uploads a media file (e.g. image, video) to the conversation. The file is uploaded (simulated here) and the S3 URL is stored as the message content.

AUTHORIZATIONS: >	JWTBearer or JWTBearer
REQUEST BODY SCHEMA: multipart/form-data	
conversation_id required	integer (Conversation Id)
file required	string <binary> (File)

Responses

> 200	Media message sent successfully
— 401	Unauthorized – invalid or missing token
— 403	User is not authorized to post in this conversation
— 422	Validation error (missing file or conversation_id)

POST /api/messages/media

Response samples

200

Content type
application/json

Copy

```
{
  "id": 0,
  "conversation_id": 0,
  "content": "string",
  "sender_sub": "string",
  "sent_at": "2019-08-24T14:15:22Z"
}
```

Rysunek 5: Dokumentacja endpointu POST /api/messages/media

2 Konfiguracja Amazon Web Services

2.1 AWS Cognito

Set up resources for your application [info](#)

► How it works

Define your application

Choose an application type and give it a name.

Application type [Info](#)

Choose the type of application that you're developing. We will show example code for application like yours.

☐ Traditional web application

An application hosted on a webserver. Uses redirects and separate pages to display information. Examples are Java, Python, nodeJS.

☒ Single-page application (SPA)

A website with a single URL that updates content based on user interaction. Examples are JavaScript, Angular, React.

☐ Mobile app

An app built with a mobile SDK. Examples are Android, iOS.

☐ Machine-to-machine application

Platform-independent server-to-server communications without user interaction. Authorizes API access with OAuth 2.0 scopes.

Name your application [Info](#)

messenger-app-cognito

Names are limited to 128 characters or fewer. Names may only contain alphanumeric characters, spaces, and the following special characters: + , . @ -

Configure options

You must make a few initial choices about the user pool that supports your application. To change these settings later, you must create a new user pool.

Options for sign-in identifiers [Info](#)

Choose sign-in attributes. Usernames can be an email address, phone number, or a user-selected username. When you select only email and phone, users must select either email or phone as their username type. When username is an option, users can sign in with any options you select if they have provided a value for that option.

☒ Email

☐ Phone number

☐ Username

Want to set up social, SAML, or OIDC sign-in?

Required attributes for sign-up [Info](#)

Choose any attributes that you want to require users to provide. With username alone, you must set email address or phone number as a required attribute.

Select attributes

email

User's preferred email address.

family_name

Surname(s) or last name(s) of the user.

given_name

Given name(s) or first name(s) of the user.

Rysunek 6: Początkowa konfiguracja tworzenia zasobów w usłudze AWS Cognito.

Edit app client information [info](#)

App clients create integration between your app and your user pool. App clients can use their own subset of authentication flows, token characteristics, and security from your user pool.

App client

Configure app clients. App clients are the user pool authentication resources attached to your app. Select an app client to configure the permitted authentication actions for an app.

App client name [Info](#)

Enter a friendly name for your app client.

messenger-app-cognito-client

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

Authentication flows [Info](#)

Choose authentication flows that your app will support. Refresh token authentication is always enabled. We have populated options based on your app type.

☐ Choice-based sign-in: ALLOW_USER_AUTH

Your user pool responds to sign-in requests with a list of available methods. Users can choose options like one-time passwords, biometric devices and security keys, and password-based sign-in with MFA.

☒ Sign in with username and password: ALLOW_USER_PASSWORD_AUTH

Users can sign in with a username and password. This method sends the username and password directly to your user pool.

☐ Sign in with secure remote password (SRP): ALLOW_USER_SRP_AUTH

Users can sign in with username and password. Your application uses SRP libraries in server-side or client-side sign-in operations to pass a password hash and verifier.

☐ Sign in with server-side administrative credentials: ALLOW_ADMIN_USER_PASSWORD_AUTH

Users can sign in with username and password in server-side authentication operations. This feature is not supported in HostedUI.

☐ Sign in with custom authentication flows from Lambda triggers: ALLOW_CUSTOM_AUTH

Users can sign in, optionally with username and password, and respond to custom challenges that you design in Lambda functions.

☒ Get new user tokens from existing authenticated sessions: ALLOW_REFRESH_TOKEN_AUTH

Your application can store a longer-lived refresh token that renews user sessions without additional user prompts.

Authentication flow session duration [Info](#)

3

minutes

Must be between 5 and 15 minutes.

Refresh token expiration [Info](#)

5

days

0

minutes

Must be between 60 minutes and 10 years.

Access token expiration [Info](#)

0

days

60

minutes

Must be between 5 minutes and 1 day. Value cannot be greater than refresh token expiration.

ID token expiration [Info](#)

0

days

60

minutes

Must be between 5 minutes and 1 day. Value cannot be greater than refresh token expiration.

Advanced security configurations - optional

☒ Enable token revocation [Info](#)

Amazon Cognito will add new claims to access and id tokens to enable revocation. This increases the size of tokens.

☒ Prevent user existence errors [Info](#)

Amazon Cognito authentication APIs return a generic authentication failure response, indicating either the user name or password is incorrect, instead of indicating that the user was not found.

Rysunek 7: Konfiguracja klienta aplikacji (App client) dla User pool.

4

Edit managed login pages configuration [info](#)

Managed login is a convenient interface for adding sign-up and sign-in to your app. The interactive managed login pages are a ready-to use authentication service and authorization server for your user pool and third-party providers.

Managed login pages
Configure the managed login pages for this app client.

Allowed callback URLs [info](#)
Enter at least one callback URL to redirect the user back to after authentication. This is typically the URL for the app receiving the authorization code issued by Cognito. You may use HTTPS URLs, as well as custom URL schemes.
URL
[Remove](#)
Length of callback URL must be between 1 and 1024 characters. Valid characters are letters, marks, numbers, symbols, and punctuation. Amazon Cognito requires HTTPS over HTTP except for http://localhost for testing purposes only. App callback URLs such as myapp://example are also supported. Must not contain a fragment.
[Add another URL](#)
You can add 99 more URLs

Allowed sign-out URLs - optional [info](#)
Enter at least one sign-out URL. The sign-out URL is a redirect page sent by Cognito when your application signs users out. This is needed only if you want Cognito to direct signed-out users to a page other than the callback URL.
URL
[Remove](#)
Length of sign-out URL must be between 1 and 1024 characters. Valid characters are letters, marks, numbers, symbols, and punctuation. Amazon Cognito requires HTTPS over HTTP except for http://localhost for testing purposes only. App sign-out URLs such as myapp://example are also supported. Must not contain a fragment.
[Add another URL](#)
You can add 99 more URLs

Identity providers [info](#)
Select the identity providers that will be available to this app client.
[+](#)

Cognito user pool [×](#)
Users can sign in to Cognito using an email, phone number, or username.

OAuth 2.0 grant types [info](#)
Choose at least one OAuth grant type to configure how Cognito will deliver tokens to this app. We have populated suggested options based on the app type you selected.

Authorization code grant [×](#)
Provides an authorization code as the response

OpenID Connect scopes [info](#)
Choose at least one OpenID Connect (OIDC) scope to specify the attributes this app client can retrieve for access tokens. We have populated suggested options based on the application type and required attributes you selected.

Email [×](#) **OpenID** [×](#) **Profile** [×](#)
Requires OpenID to be selected

Custom scopes [info](#)
Select custom scopes that you will authorize for this app. Custom scopes are configured with resource servers.
[+](#)

Rysunek 8: Konfiguracja zarządzanej strony logowania.

2.2 AWS S3

Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [info](#)

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

Rysunek 9: Tworzenie nowego zasobu typu bucket w usłudze Amazon S3.

Object Ownership

Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Rysunek 10: Konfiguracja własności obiektów i dostępu publicznego.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Tags - optional (2)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key

Project

Value - optional

messenger-app

Remove

Environment

prod

Remove

Add tag

Default encryption

Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type

Info

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☒ Disable

☐ Enable

Rysunek 11: Konfiguracja wersjonowania, tagowania i szyfrowania.

6

2.3 AWS RDS

Create database [Info](#)


Choose a database creation method


☒ **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 15.10-R1

☐ Enable RDS Extended Support [Info](#)
Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for PostgreSQL documentation](#).

Rysunek 12: Wybór silnika i wersji bazy danych PostgreSQL podczas tworzenia instancji RDS.

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.

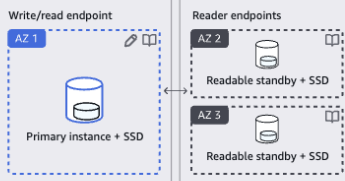
☒ **Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

Availability and durability

Deployment options [Info](#)
Choose the deployment option that provides the availability and durability needed for your use case. AWS is committed to a certain level of uptime depending on the deployment option you choose. Learn more in the [Amazon RDS service level agreement \(SLA\)](#).

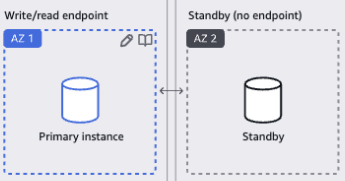
☐ **Multi-AZ DB cluster deployment (3 instances)**
Creates a primary DB instance with two readable standbys in separate Availability Zones. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones
- Increased read capacity
- Reduced write latency




☐ **Multi-AZ DB instance deployment (2 instances)**
Creates a primary DB instance with a non-readable standby instance in a separate Availability Zone. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones



☒ **Single-AZ DB instance deployment (1 instance)**
Creates a single DB instance without standby instances. This setup provides:

- 99.5% uptime
- No data redundancy



Rysunek 13: Wybór szablonu i strategii wdrożenia instancji bazy danych w Amazon RDS.

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.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 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.

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.

☐ **Auto generate password**
 Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Password strength Weak

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

Rysunek 14: Konfiguracja identyfikatora instancji oraz danych logowania do bazy danych.

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)
▼ Hide filters

☐ Include previous generation classes

☐ Standard classes (includes m classes)
 ☐ Memory optimized classes (includes r and x classes)
 ☒ Burstable classes (includes t classes)

2 vCPUs 1 GiB RAM Network: Up to 2085 Mbps

Storage

Storage type [Info](#)
 Provisioned IOPS SSD (io2) storage volumes are now available.

Baseline performance determined by volume size

Allocated storage [Info](#)

GiB

Allocated storage value must be 20 GiB to 6144 GiB

▼ Additional storage configuration

Storage autoscaling [Info](#)
 Provides dynamic scaling support for your database's storage based on your application's needs.

☐ **Enable storage autoscaling**
 Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Rysunek 15: Wybór klasy instancji oraz konfiguracja przestrzeni dyskowej dla bazy danych.

Connectivity
Info

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

☒ **Don't connect to an EC2 compute resource**
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

☐ **Connect to an EC2 compute resource**
Set up a connection to an EC2 compute resource for this database.

Network type Info
To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

☒ **IPv4**
Your resources can communicate only over the IPv4 addressing protocol.

☐ **Dual-stack mode**
Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

messenger-app-vpc (vpc-032b09061a08d75a6)
3 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change its VPC.

DB subnet group Info
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

Create new DB Subnet Group

Rysunek 16: Konfiguracja sieciowa instancji bazy danych: wybór sieci VPC oraz grupy podsieci.

Public access Info
☐ **Yes**
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
☒ **No**
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ **Choose existing**
Choose existing VPC security groups

☐ **Create new**
Create new VPC security group

Existing VPC security groups
Choose one or more options

messenger-app-vpc-backend-sg X messenger-app-vpc-database-sg X

Availability Zone Info
No preference

RDS Proxy
RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.
☐ **Create an RDS Proxy** Info
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

Certificate authority - optional Info
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)
Expiry: May 26, 2061

If you don't select a certificate authority, RDS chooses one for you.

Additional configuration
Database port Info
TCP/IP port that the database will use for application connections.

5432

Rysunek 17: Ustawienia dostępu oraz przypisanie grupy zabezpieczeń dla instancji bazy danych.

Monitoring [info](#)

Choose monitoring tools for this database. Database Insights provides a combined view of Performance Insights and Enhanced Monitoring for your fleet of databases. **Database Insights** pricing is separate from RDS monthly estimates. See [Amazon CloudWatch pricing](#).

☐ Database Insights - Advanced

- Retains 15 months of performance history
- Fleet-level monitoring
- Integration with CloudWatch Application Signals

☒ Database Insights - Standard

- Retains 7 days of performance history, with the option to pay for the retention of up to 24 months of performance history

Performance Insights

☐ Enable Performance insights

With Performance Insights dashboard, you can visualize the database load on your Amazon RDS DB instance load and filter the load by waits, SQL statements, hosts, or users.

▼ Additional monitoring settings

Enhanced Monitoring, CloudWatch Logs and DevOps Guru

Enhanced Monitoring

☐ Enable Enhanced monitoring

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Log exports

Select the log types to publish to Amazon CloudWatch Logs

☐ iam-db-auth-error log
☒ PostgreSQL log
☐ Upgrade log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Rysunek 18: Konfiguracja monitoringu oraz dla instancji bazy danych.

▼ Additional configuration

Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name [Info](#)

messenger_app_db

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.postgres15

Option group [Info](#)

default:postgres-15

Backup

☐ Enable automated backups

Creates a point-in-time snapshot of your database

Encryption

☐ Enable encryption

Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Maintenance

Auto minor version upgrade [Info](#)

☐ Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

☐ Choose a window
☒ No preference

Deletion protection

☐ Enable deletion protection

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Rysunek 19: Dodatkowa konfiguracja instancji – backup, szyfrowanie, konserwacja i ochrona.

2.4 AWS Elastic Beanstalk

Configure environment [Info](#)

Environment tier [Info](#)

Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

- ☒ **Web server environment**
Run a website, web application, or web API that serves HTTP requests. [Learn more](#)
- ☐ **Worker environment**
Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#)

Application information [Info](#)

Application name

messenger-app-backend

Maximum length of 100 characters.

▼ Application tags (optional)

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

Key

Q Environment



Q Project



Add new tag

You can add 48 more tags.

Value - optional

Q prod



Remove

Q messenger-app



Remove

Rysunek 20: Konfiguracja środowiska aplikacji backendowej w Amazon Elastic Beanstalk.

Environment information [Info](#)

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

messenger-app-backend-env

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.

Domain

Leave blank for autogenerated value

.us-east-1.elasticbeanstalk.com

Check availability

Environment description

Production backend environment for Messenger App

Platform [Info](#)

Platform type

- ☒ **Managed platform**
Platforms published and maintained by Amazon Elastic Beanstalk. [Learn more](#)
- ☐ **Custom platform**
Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

Docker



Platform branch

Docker running on 64bit Amazon Linux 2



Platform version

4.1.0 (Recommended)



Rysunek 21: Ustawienia środowiska backendowego - nazwa środowiska i platforma Docker.

Application code [Info](#)

☐ Sample application

☐ Existing version
Application versions that you have uploaded.

☒ Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

Version label
Unique name for this version of your application code.

deploy-v1

Source code origin. Maximum size 500 MB

☐ Local file

☒ Public S3 URL

https://messenger-app-artifacts.s3.us-east-1.amazonaws.com/messenger-app-backend.zip

Presets [Info](#)

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets

☐ Single instance (free tier eligible)

☐ Single instance (using spot instance)

☐ High availability

☐ High availability (using spot and on-demand instances)

☒ Custom configuration

Rysunek 22: Wgranie wersji aplikacji z pliku na S3 oraz wybór konfiguracji środowiska.

Configure service access [Info](#)

Service access

IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. [Learn more](#)

Service role

☐ Create and use new service role

☒ Use an existing service role

Existing service roles

Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.

LabRole

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. [Learn more](#)

vockey

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

LabInstanceProfile

View permission details

Rysunek 23: Konfiguracja ról IAM oraz pary kluczy EC2 dla środowiska backendowego.

Set up networking, database, and tags - optional [Info](#)

Virtual Private Cloud (VPC)

VPC

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console. [Learn more](#)

vpc-0c0aaf16d6771abe7 | (10.0.0.0/16) | messenger-app-vpc

Create custom VPC

Instance settings

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. [Learn more](#)

Public IP address

Assign a public IP address to the Amazon EC2 instances in your environment.

☒ Activated

Instance subnets

Filter instance subnets

	Availability Zone	Subnet	CIDR	Name
<input type="checkbox"/>	us-east-1a	subnet-0372fb6b1085b9f66	10.0.1.0/24	messenger-app-vpc-frontend-subnet
<input checked="" type="checkbox"/>	us-east-1b	subnet-0b41df935191e2aee	10.0.2.0/24	messenger-app-vpc-backend-subnet
<input type="checkbox"/>	us-east-1c	subnet-0ebfc5d0ca5791917	10.0.3.0/24	messenger-app-vpc-database-subnet

Rysunek 24: Konfiguracja sieci VPC oraz podsieci dla instancji środowiska backendowego.

Configure instance traffic and scaling - optional [Info](#)

Instances

Info

Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type

(Container default)

Size

The number of gigabytes of the root volume attached to each instance.

GB

IOPS

Input/output operations per second for a provisioned IOPS (SSD) volume.

IOPS

Throughput

The desired throughput to provision for the Amazon EBS root volume attached to your environment's EC2 instance

125

MiB/s

Amazon CloudWatch monitoring

The time interval between when metrics are reported from the EC2 instances

Monitoring interval

5 minute

Instance metadata service (IMDS)

Your environment's platform supports both IMDSv1 and IMDSv2. To enforce IMDSv2, deactivate IMDSv1. [Learn more](#)

IMDSv1

With the current setting, the environment enables only IMDSv2.

☒ Deactivated

EC2 security groups

Select security groups to control traffic.

EC2 security groups (3)

Filter security groups

	Group name	Group ID	Name
<input type="checkbox"/>	default	sg-0cd9d32807fdc8ab2	
<input checked="" type="checkbox"/>	messenger-app-vpc-backend-sg	sg-041da23276cf889f7	
<input type="checkbox"/>	messenger-app-vpc-database-sg	sg-035f1b100305e63bf	

Rysunek 25: Konfiguracja instancji EC2, grup zabezpieczeń oraz ustawień monitorowania.

13

▼ Capacity [Info](#)
Configure the compute capacity of your environment and auto scaling settings to optimize the number of instances used.

Auto scaling group

Environment type
Select a single-instance or load-balanced environment. You can develop and test an application in a single-instance environment to save costs and then upgrade to a load-balanced environment when the application is ready for production. [Learn more](#)

Load balanced

Instances

1 Min

1 Max

Fleet composition
Spot instances are launched at the lowest available price. [Learn more](#)

☒ On-Demand instances

☐ Combine purchase options and instances

Rysunek 26: Konfiguracja typu środowiska, liczby instancji oraz autoskalowania.

Architecture
The processor architecture determines the instance types that are made available. You can't change this selection after you create the environment. [Learn more](#)

☒ x86_64
This architecture uses x86 processors and is compatible with most third-party tools and libraries.

☐ arm64 - new
This architecture uses AWS Graviton2 processors. You might have to recompile some third-party tools and libraries.

Instance types
Add instance types for your environment with your preferred launch order. The order preference only applies to On-Demand instances and Spot instances that use the capacity optimized prioritized allocation strategy. We recommend you include at least two instance types. [Learn more](#)

1. t3.micro

Add instance type

Rysunek 27: Wybór architektury procesora oraz typu instancji EC2.

Load balancer network settings

Visibility
Make your load balancer internal if your application serves requests only from connected VPCs. Public load balancers serve requests from the Internet.

Public

Load balancer subnets

Filter load balancer subnets

	Availability Zone	Subnet	CIDR	Name
<input type="checkbox"/>	us-east-1a	subnet-0372fb6b1085b9f66	10.0.1.0/24	messenger-app-vpc-frontend-subnet
<input checked="" type="checkbox"/>	us-east-1b	subnet-0b41df935191e2aee	10.0.2.0/24	messenger-app-vpc-backend-subnet
<input type="checkbox"/>	us-east-1c	subnet-0ebfc5d0ca5791917	10.0.3.0/24	messenger-app-vpc-database-subnet

Load Balancer Type

☒ Application load balancer
Application layer load balancer—routing HTTP and HTTPS traffic based on protocol, port, and route to environment processes.

☐ Classic load balancer
Previous generation — HTTP, HTTPS, and TCP

☐ Network load balancer
Ultra-high performance and static IP addresses for your application.

☒ Dedicated
Use a load balancer that Elastic Beanstalk creates exclusively for this environment.

☐ Shared
Use a load balancer that someone in your account created. It can be shared among multiple Elastic Beanstalk environments.

Listeners
You can specify listeners for your load balancer. Each listener routes incoming client traffic on a specified port using a specified protocol to your environment processes. By default, we've configured your load balancer with a standard web server on port 80.

Actions Add listener

	Listener Port	Listener Protocol	SSL certificate	Default process	Enabled
<input type="radio"/>	443	HTTPS	arn:aws:acm:us-east-1:84958...	default	<input checked="" type="checkbox"/>
<input type="radio"/>	80	HTTP	—	default	<input checked="" type="checkbox"/>

Rysunek 28: Konfiguracja ustawień sieciowych i listenerów Load Balancera.

Configure updates, monitoring, and logging - optional [Info](#)

▼ Monitoring [Info](#)

Health reporting

Enhanced health reporting provides free real-time application and operating system monitoring of the instances and other resources in your environment. The **EnvironmentHealth** custom metric is provided free with enhanced health reporting. Additional charges apply for each custom metric. For more information, see [Amazon CloudWatch Pricing](#).

System

- ☐ Basic
☒ Enhanced

CloudWatch Custom Metrics - Instance

Choose metrics

CloudWatch Custom Metrics - Environment

Choose metrics

Health monitoring rule customization

Configure the HTTP application and load balancer status codes included in determining your environment's health. [Learn more](#)

Ignore application 4xx

☒ Activated

Ignore load balancer 4xx

☒ Activated

Health event streaming to CloudWatch Logs

Configure Elastic Beanstalk to stream environment health events to CloudWatch Logs. You can set the retention up to a maximum of ten years and configure Elastic Beanstalk to delete the logs when you terminate your environment.

Log streaming

☒ Activated (standard CloudWatch charges apply.)

Retention

7

Lifecycle

Delete logs upon termination

Rysunek 29: Konfiguracja monitoringu, logowania i raportowania stanu.

▼ Platform software [Info](#)

Configure the options available to your specific platform. These include the proxy server and OS environment properties. [Learn more](#)

Container options

Proxy server

Nginx

Amazon X-Ray

Amazon X-Ray is a service that collects data about the requests and responses that your application serves and receives. You can use the tools that X-Ray offers to view and filter the data that it provides to identify potential issues and optimization opportunities.

X-Ray daemon

(service charges may apply.)

☒ Activated

S3 log storage

Configure the instances in your environment to upload rotated logs to Amazon S3. [Learn more](#)

Rotate logs

(standard S3 charges apply.)

☒ Activated

Instance log streaming to CloudWatch logs

Configure the instances in your environment to stream logs to CloudWatch logs. You can set the retention up to 10 years and configure Elastic Beanstalk to delete the logs when you terminate your environment. [Learn more](#)

Log streaming

(standard CloudWatch charges apply.)

☒ Activated

Retention

7

Lifecycle

Delete logs upon ter...

Rysunek 30: Konfiguracja oprogramowania platformy - proxy, logi i X-Ray.

2.5 AWS CloudWatch

Log groups (13)

By default, we only load up to 10000 log groups.



Filter log groups or try prefix search

Exact match

<input type="checkbox"/>	Log group	Log class	Anomaly d...
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/docker	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/docker-compose-events.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/docker-events.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-docker/containers/eb-current-app/stdouterr.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-docker/containers/eb-current-app/unexpected-quit.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-engine.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-hooks.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/nginx/access.log	Standard	Configure
<input type="checkbox"/>	/aws/elasticbeanstalk/messenger-app-backend-env/var/log/nginx/error.log	Standard	Configure

Rysunek 31: Grupy logów aplikacji backendowej w usłudze Amazon CloudWatch.

/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-docker/containers/eb-current-app/stdouterr.log

Actions

View in Logs Insights

Start tailing

Search log group

Log group details

Log class
Standard

ARN

arn:aws:logs:us-east-1:849581805532:log-group:/aws/elasticbeanstalk/messenger-app-backend-env/var/log/eb-docker/containers/eb-current-app/stdouterr.log:*

Creation time

1 hour ago

Retention

1 week

Stored bytes

-

Metric filters

0

Subscription filters

0

Contributor Insights rules

-

KMS key ID

-

Anomaly detection

[Configure](#)

Data protection

-

Sensitive data count

-

Field indexes

[Configure](#)

Transformer

[Configure](#)

Log streams

Tags

Anomaly detection

Metric filters

Subscription filters

Contributor Insights

Data protection

Field indexes - new

Transformer - new

Log streams (2)

Filter log streams or try prefix search

Exact match Show expired Info



Delete

Create log stream

Search all log streams

Log stream



Last event time



☐

[i-043fa538abd33fac7](#)

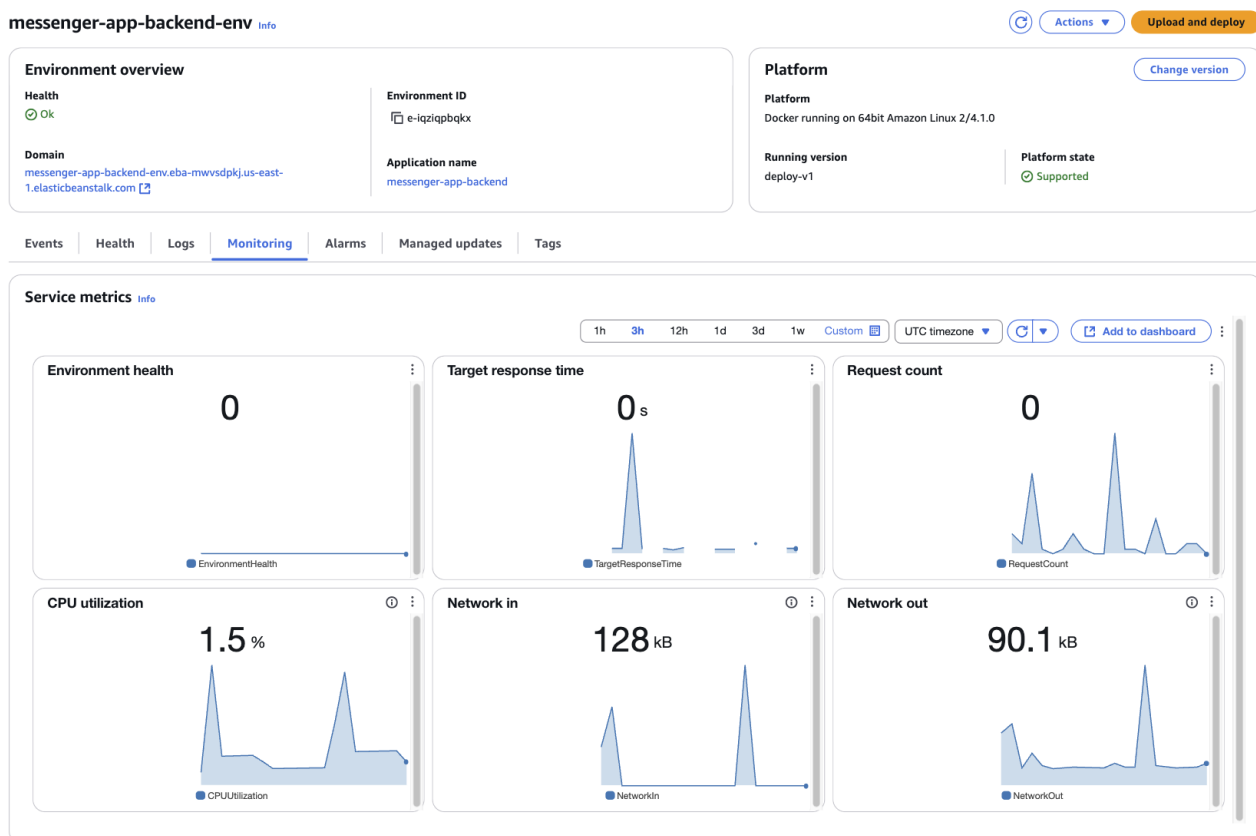
2025-04-06 10:12:38 (UTC)

☐

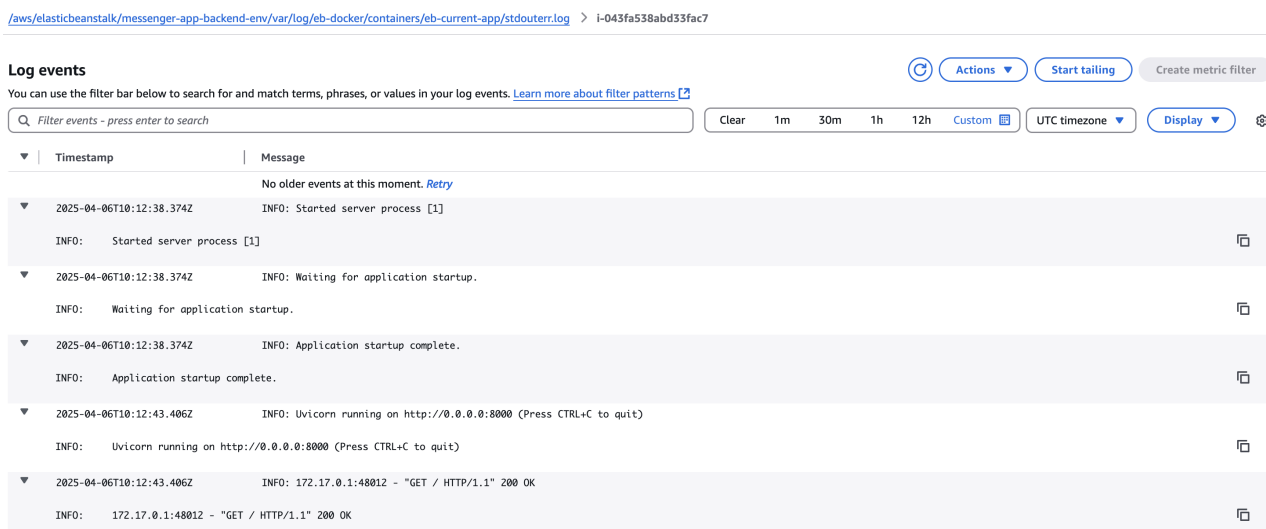
[i-0ba48fc399dc303f7](#)

2025-04-06 09:50:44 (UTC)

Rysunek 32: Lista dostępnych strumieni logów aplikacji backendowej w grupie logów stdouterr.



Rysunek 33: Panel monitorowania środowiska backendowego w Amazon Elastic Beanstalk.



Rysunek 34: Zawartość strumienia logów aplikacji backendowej - logi z serwera FastAPI.