

Тема: Разгръщане на проекта по уеб технологии в AWS - Статистика за използвани медии

Предмет: Приложно-програмни интерфейси за работа с облачни архитектури с Амазон Уеб Услуги (AWS)

Изготвил: Димитър Калмадански, фн: 81758,
имейл:dimitar_eco@abv.bg

Лектор: проф. д-р Милен Петров, година: 2023

Съдържание

1	Условие	2
2	Въведение	2
3	Теория	2
4	Използвани технологии	3
5	Инсталация и настройки	4
6	Кратко ръководство за потребителя	14
7	Примерни данни	17
8	Описание на програмния код	17
9	Приноси на студента, ограничения и възможности за бъдещо развитие	17
10	Какво научих	17
11	Списък с фигури	17
12	Използвани източници	18

1 Условие

Да се разгърне проектът, изготвен по време на курса по Уеб технологии, като се използват AWS услуги - поне една обща и една специфична.

2 Въведение

AWS стартира като част от Amazon през 2002 и през 2006 вече има изчислителни услуги в облака. Оттогава се добавят нови и постоянно се разрастват, което ги прави едни от водещите в индустрията.

С предлаганите услуги може да се качи динамичен сайт на уеб сървър, позволяващ бърз и сигурен достъп от целия свят; да се ограничи достъпът в частно виртуално пространство, да се управлява базата от данни към сървъра, да защитим сайта ни от злонамерени атаки и т.н.

3 Теория

Конфигурацията за услугите е в секция "Инсталация и настройки" и "Кратко ръководство за потребителя".

В проекта е използвана EC2 услугата като сървър за сайта. Конфигурацията е в секция "Инсталация и настройки". Повече информация за услугата може да намерите на официалния сайт:

<https://aws.amazon.com/ec2/>

Връзка със самата EC2 инстанция от конзолата се осъществява с SSH протокол в Windows PowerShell. Може да се инсталира от сайта на Windows:

<https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.3>

Като база от данни е използвана RDS услугата с engine MariaDB. Повече информация за услугата може да намерите на официалния сайт:

<https://aws.amazon.com/rds/>

За съхранение на файловете за сайта като backup е използван S3 bucket без публичен достъп. Повече информация за услугата може да намерите на официалния сайт:

<https://aws.amazon.com/s3/>

Като частна мрежа в облака, осигуряваща достъп до сървъра и комуникация между него и базата данни, е използвана VPC. Повече информация за услугата може да намерите на официалния сайт:

<https://aws.amazon.com/vpc/>

За достъп на сървъра до файловете в S3 bucket е използвана IAM роля на съответния сървис. Повече за как се създават и ползват ролите може да видите тук:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html

За връзка и управление на базата от данни е използван PHPMyAdmin 5.2.1. Повече информация за софтуера може да намерите на официалния сайт:
<https://www.phpmyadmin.net/>

4 Използвани технологии

Като сървър за вече разработения сайт е използван Amazon Linux 2 AMI на EC2:

- **EC2** - amzn2-ami-kernel-5.10-hvm-2.0.20230504.1-x86_64-gp2

Свързана е и база от данни към сървъра, върху която се изпълняват SQL заявки. За управлението се ползва RDS услугата:

- **RDS** - MariaDB 10.6.10 engine, 20 Gib SSD (gp2)

Използван е S3 bucket за първоначалното качване на файловете на сайта за трансфер на сървъра.

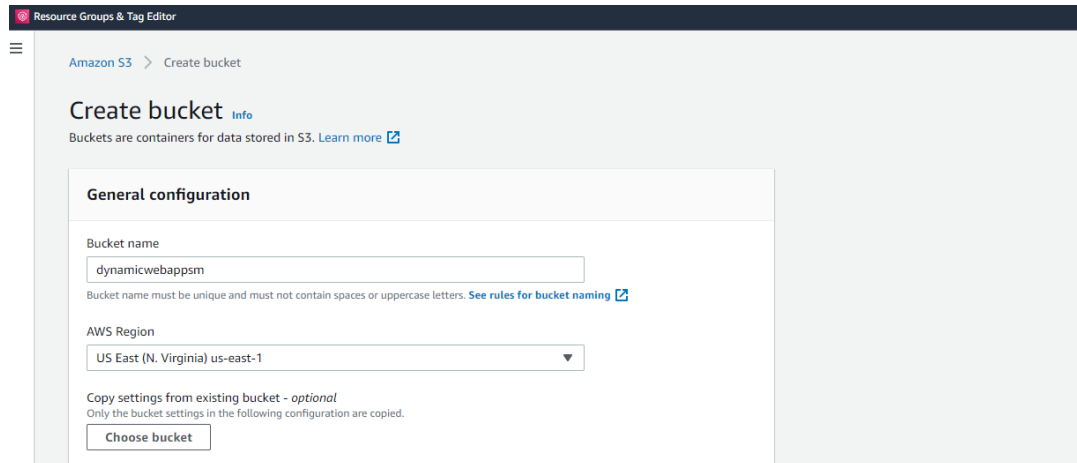
- **S3** - EU (Frankfurt) eu-central-1 регион, Standard storage class за файловете

Създаден е частен виртуален облак за сигурност и контрол на EC2, RDS инстанциите и достъпа до тях.

- **VPC** - регион EU (Frankfurt) с 3 подмрежи в 3 availability зони за RDS и 1 подмрежа в 1 availability зона за EC2

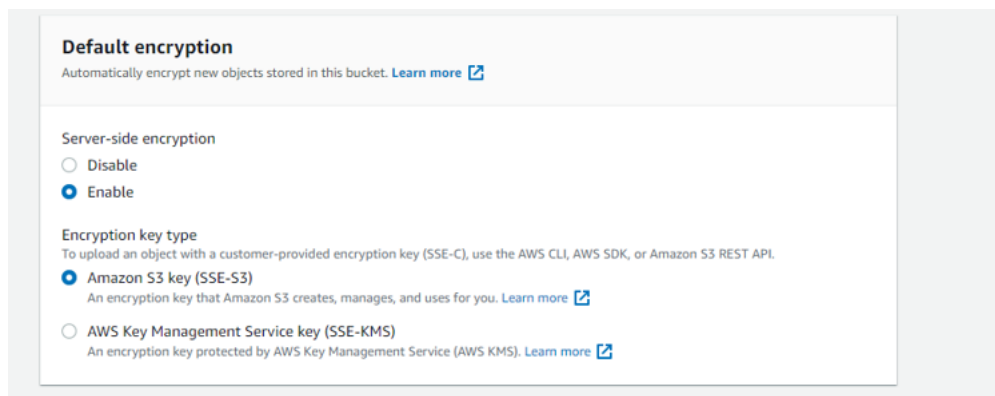
5 Инсталация и настройки

- Отидете до S3 сървиса в AWS конзолата
- Изберете име за S3 bucket, като му дадете уникално глобално име и изберете подходящ регион (където ще е сървърът)



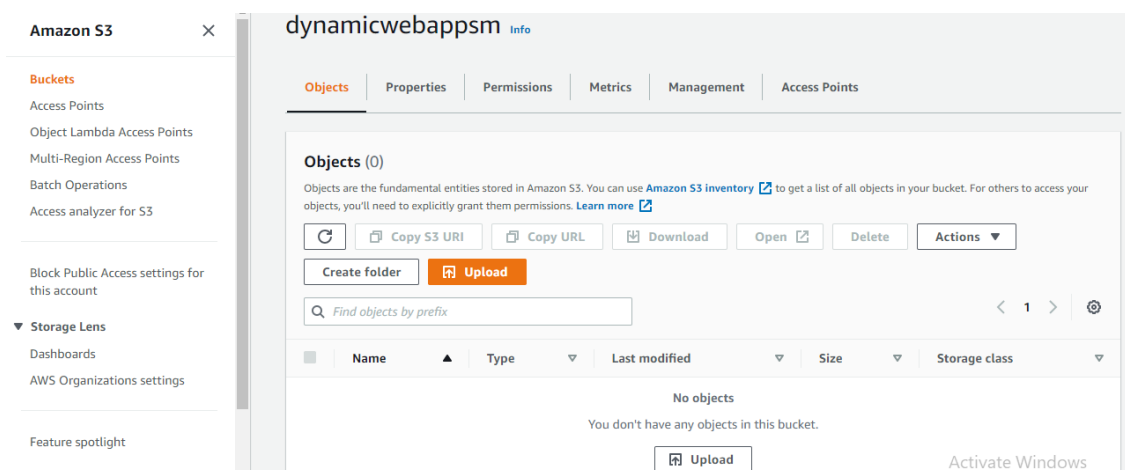
Фигура 1: Избиране на име и регион за bucket

- Изберете "Block all public" на Block Public Access settings
- Изберете "Disable" за Bucket Versioning
- Изберете "Enable" за Server-side encryption и за ключ ползвайте Amazon S3 Key (SSE-S3)



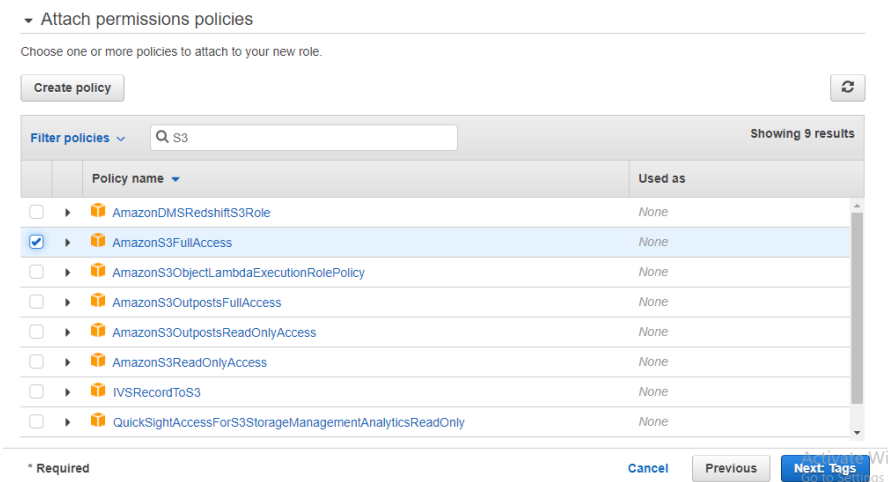
Фигура 2: Избиране на настройки за енкриптиране на обекти в bucket

Качете директорията с всички файлове за сайта, като отидете на Objects и ползвате Upload



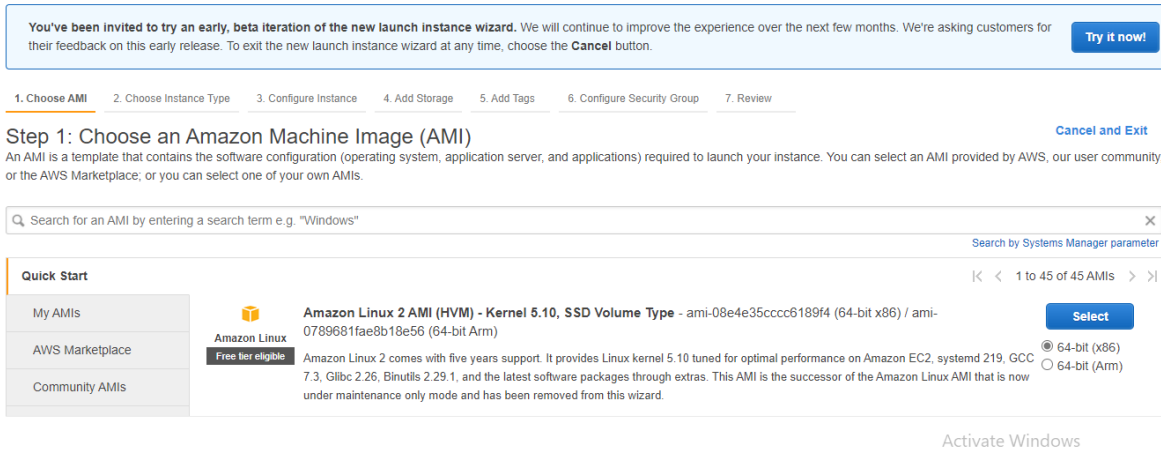
Фигура 3: Качване на файлове в създадения bucket

- Отидете на IAM сървиса за създаване на роля
- Изберете EC2 като опция
- Намерете политика AmazonS3FullAccess и я селектирайте



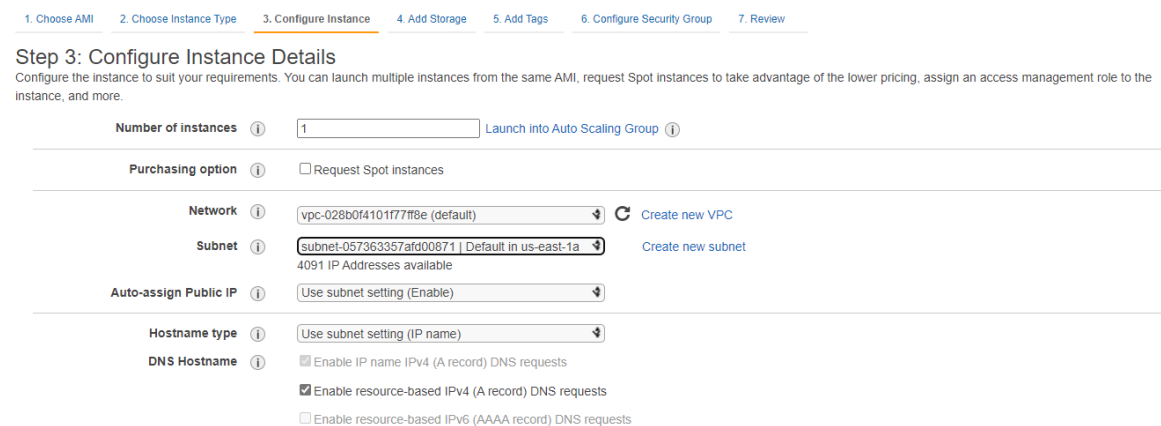
Фигура 4: Избиране на политика за достъп на EC2 до S3 обекти

- Дайте й име и описание и продължете
- Отидете на EC2 сървиса за пускане на сървърна инстанция
- За AMI изберете Amazon Linux 2 (HVM), достъпно за Free Tier



Фигура 5: Избиране на AMI за EC2

- За тип инстанция ползвайте t2.micro
- При конфигурация на детайли изберете Default VPC и използвайте създадената подмрежа по подразбиране



Фигура 6: Избиране на VPC за EC2

- Изберете за роля на инстанцията тази, която създадохте по-рано
- При добавяне на памет ползвайте по подразбиране SSD (gp2) 8 GB за EBS

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0c03ce90cef384dca	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

▼ Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Фигура 7: Добавяне на памет EBS към EC2

- Добавете тагове по желание
- Създайте нова security група и добавете следните 3 правила на Inbound rules
 - HTTP и HTTPS за IPv4 като източник е всяко IP
 - SSH за IPv4 като източник е вашето IP

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

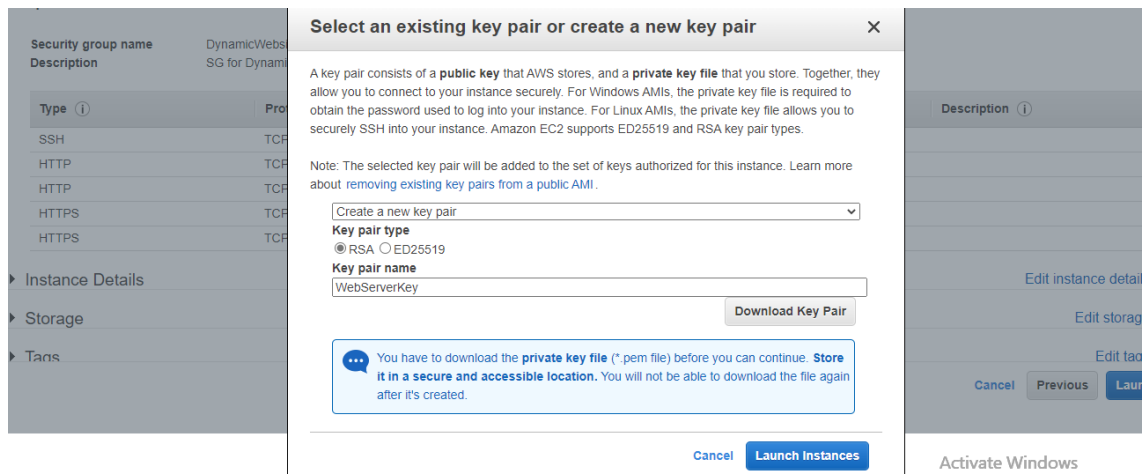
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 197.42.126.153/32	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Anywhere 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

[Add Rule](#)

[Cancel](#) [Previous](#) [Review and Launch](#)

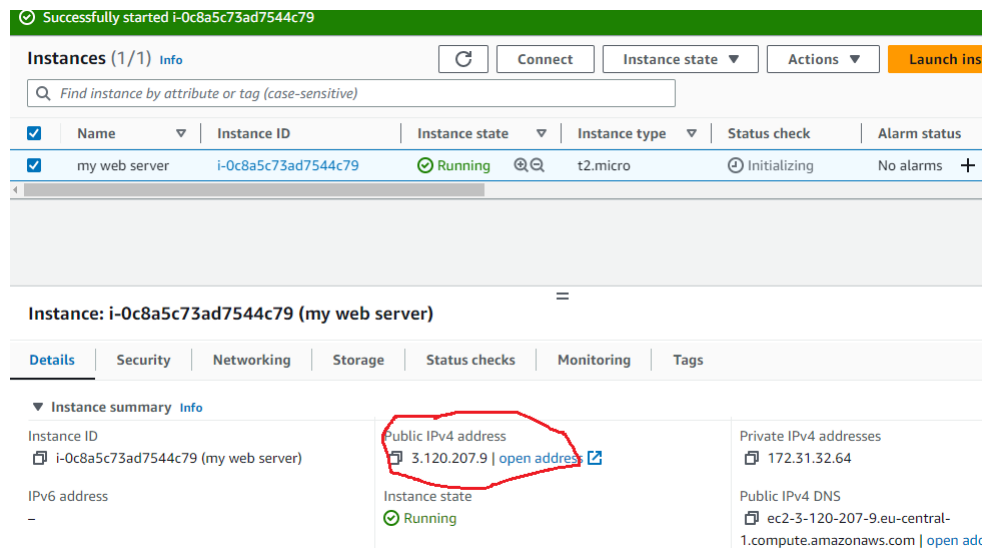
Фигура 8: Добавяне на правила в security групата на инстанцията

- Създайте нов key pair, за да се свързвате към EC2 инстанцията и го запазете на компютъра



Фигура 9: Създаване на key pair за достъп до EC2

- Стартирайте EC2 инстанцията



Фигура 10: Стартирана EC2 инстанция с публично IPv4

- Стартирайте Windows PowerShell
- Въведете вашите данни в следния код за свързване с инстанцията:
`ssh -i <път до key pair> <EC2 име на потребител>@<публичен адрес на EC2>`
 Пример: `ssh -i C:\Users\offline\Desktop\mykeypair.pem ec2-user@3.120.207.9`
- Ако бъдете попитани за потвърждение при първо свързване до инстанцията, напишете **yes**
- Направете ъпдейт на софтуерните компоненти на сървъра за всеки случай
`sudo yum update -y`


```

The authenticity of host '3.120.207.9 (3.120.207.9)' can't be established.
ECDSA key fingerprint is SHA256:lyehWI5bI6nnzRhqBVdOnOq+JmIyGRZae8LXjJjCwyY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.120.207.9' (ECDSA) to the list of known hosts.
Last login: Fri Jun  2 09:33:19 2023 from 84.40.100.145

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-32-64 ~]$ █

```

Фигура 11: Свързване с EC2 в Windows PowerShell

- Инсталирайте LAMP, MariaDB и PHP репотата от Amazon Linux Extras за най-новите версии
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
- Инсталирайте Apache сървър, MariaDB и PHP
sudo yum install -y httpd mariadb-server
- Стартирайте Apache сървър
sudo systemctl start httpd
- По желание конфигурирайте сървър да почва след всяко стартиране на системата
sudo systemctl enable httpd
- Изпълнете следната команда за копиране на файловете от S3 бъкета в директория за вашия сървър
sudo aws s3 cp <адрес на бъкет> -region <име на регион> /var/www/html/ -recursive
 Пример: **sudo aws s3 cp s3://fmibucket1234 -region eu-central-1 /var/www/html/ -recursive**
- Проверете дали файловете са правилно копирани
cd /var/www/html
ls
 Трябва да видите името на папката с файловете за сайта
- Отидете до RDS сървиса за създаване на база данни
- Като метод за създаване изберете Standard create и като engine ползвайте MariaDB
- Селектирайте най-новата версия, в случая 10.6.10, Free Tier за шаблон и изберете име за базата


Choose a database creation method [Info](#)


☒ **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)


☐ Aurora (PostgreSQL Compatible)


☐ MySQL


☒ **MariaDB**


☐ PostgreSQL


☐ Oracle


Фигура 12: Избиране на тип база от данни за сървъра

Engine version

MariaDB 10.6.10 ▼

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](#)

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.

mydatabase2

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.

Фигура 13: Избиране на версия и име на базата

- Изберете име и парола за достъп до базата и ги запомнете
- Като тип на инстанцията изберете db.t3.micro

▼ **Credentials Settings**

Master username [Info](#)
Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

☐ **Manage master credentials in AWS Secrets Manager**
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

[i](#) If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
[Learn more](#) [↗](#)

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

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm master password [Info](#)

Фигура 14: Избор на име и парола за вход в базата

- За тип памет General Purpose SSD (gp2) с 20 GiB, autoscaling по желание

Storage

Storage type [Info](#)

Baseline performance determined by volume size ▼

Allocated storage [Info](#)

GiB

The minimum value is 20 GiB and the maximum value is 6,144 GiB

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.

Maximum storage threshold [Info](#)
Charges will apply when your database autoscales to the specified threshold

GiB

The minimum value is 22 GiB and the maximum value is 6,144 GiB

Фигура 15: Избор на памет за базата

- На Connectivity ще свържем базата с EC2 инстанцията, която вече сме създали

Availability & durability

Multi-AZ deployment [Info](#)

☐ Create a standby instance (recommended for production usage)
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

☐ Do not create a standby instance

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.

EC2 instance [Info](#)
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i-0c8a5c73ad7544c79
my web server ▼ ↻

Фигура 16: Свързване на базата със сървъра

- Изберете същото VPC, в което се намира EC2 - трябва да е Default в случая; за DB subnet group използвайте Automatic setup

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.

Default VPC (vpc-07e186a609a52be0c) ▼
4 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.

☐ Choose existing
Choose existing DB subnet group

☒ **Automatic setup**
RDS creates a new subnet group for you or reuses an existing subnet group

DB subnet group name

rds-ec2-db-subnet-group-2 ▼

Фигура 17: Избиране на VPC и създаване на подмрежова група за базата

- Достъпът няма да е публичен, за security група използвайте новосъздадената от Амазон от тип rds-ec2. Тя ще се прикрепи за базата за достъп на EC2 до нея

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

Additional VPC security group

Choose one or more options ▼

rds-ec2-1 ✕

Amazon RDS will add a new VPC security group *rds-ec2-3* to allow connectivity with your compute resource.

Фигура 18: Прикачване на групата към RDS инстанцията

- AZ трябва в случая да е същата, в която се намира EC2. Портът е 3306, използваме автентикация с парола само

Availability Zone [Info](#)

eu-central-1b ▼

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-2019 (default) ▼

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.

3306

Database authentication

Database authentication options [Info](#)

☒ **Password authentication**
Authenticates using database passwords.

☐ **Password and IAM database authentication**
Authenticates using the database password and user credentials through AWS IAM users and roles.

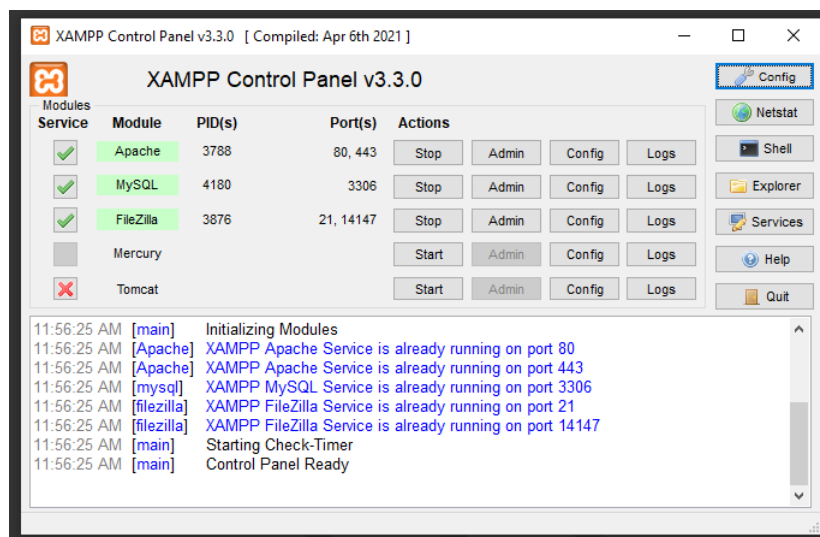
Фигура 19: Избор на автентикация с базата, зона и порт

Прикачената към RDS инстанцията security група служи за свързване на EC2, ако определена група е прикачена към него. Има 1 inbound правило само от тип MySQL/Aurora.

Прикачената към EC2 група позволява свързване с базата от данни. Има 1 outbound правило само от тип MySQL/Aurora.

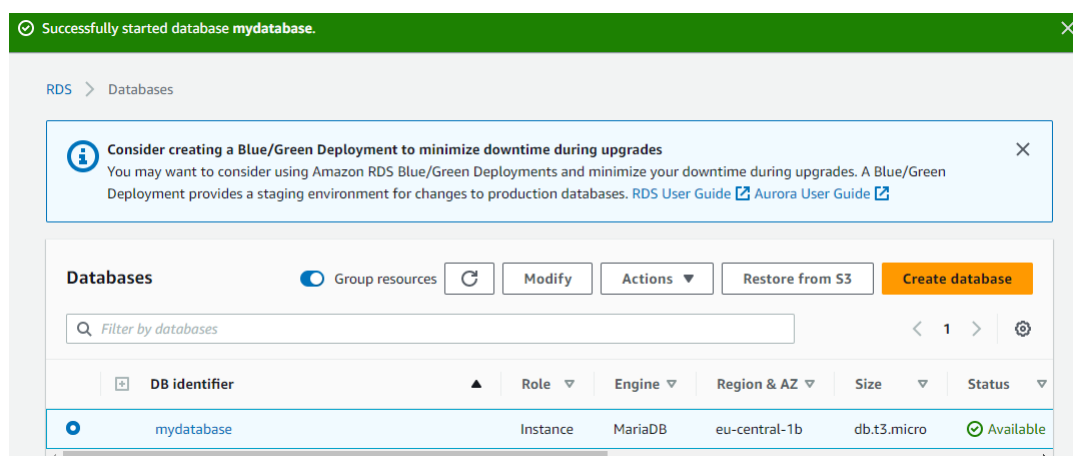
6 Кратко ръководство за потребителя

- Стартирайте XAMPP контролен панел и пуснете Apache, MySQL сървисите

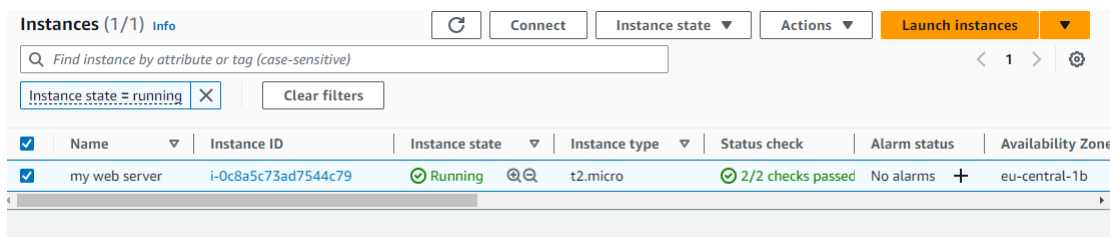


Фигура 20: XAMPP контролен панел със стартиран сървър

- Стартирайте EC2 и RDS инстанциите от AWS конзолата



Фигура 21: Стартирана RDS база



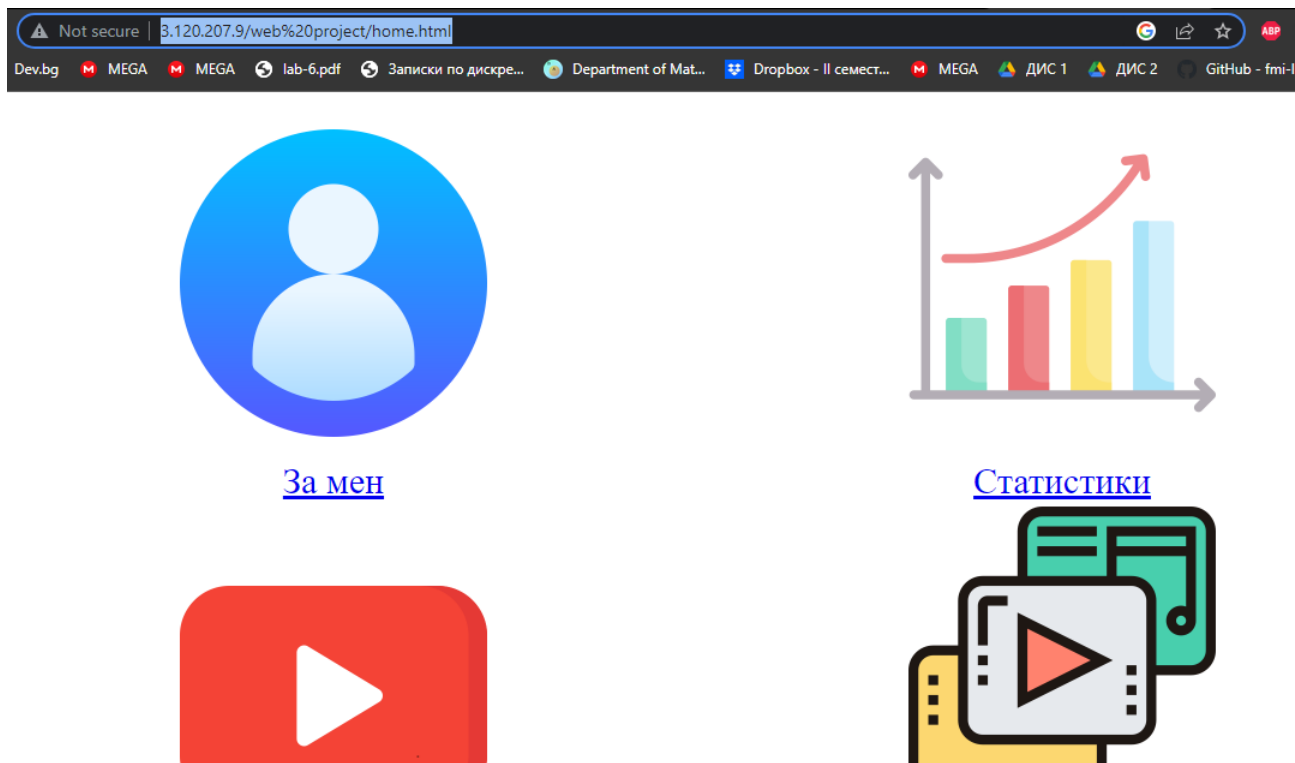
Фигура 22: Стартиран EC2

- Свържете се с EC2 инстанцията от Windows PowerShell

- Създайте нова директория за PHPMyAdmin за управление на базата данни
sudo mkdir -p /var/www/html/phpmyadmin
- Свалете пакета с най-новата версия на PHPMyAdmin от сайта
wget https://files.phpmyadmin.net/phpMyAdmin/5.2.1/phpMyAdmin-5.2.1-all-languages.tar.gz
- Разархивирайте пакета в папката
sudo tar -xvf phpMyAdmin-5.2.1-all-languages.tar.gz -C /var/www/html/phpmyadmin
- Навигирайте до файловете за PHPMyAdmin
**cd phpmyadmin/
cd phpMyAdmin-5.2.1-all-languages/**
- Отворете конфигурационния файл с редактор
sudo vim config.sample.inc.php
- Добавете следните редове по този начин за настройки на сървъра след Server parameters, ако липсват

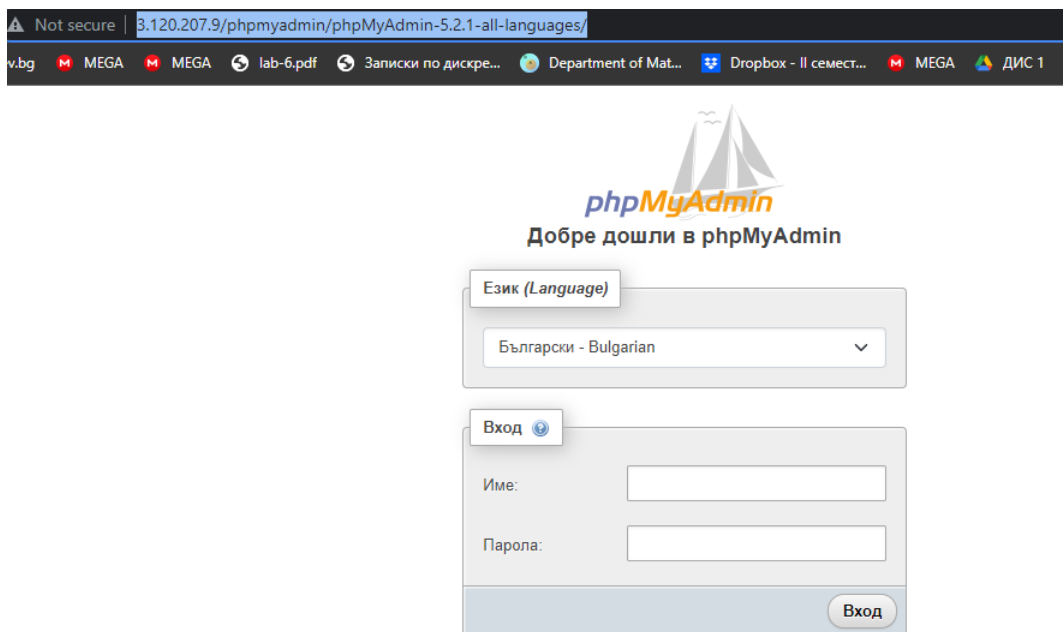
```
cfg['Servers'][$i]['host'] = <endpoint на базата от AWS>;  
cfg['Servers'][$i]['compress'] = false;  
cfg['Servers'][$i]['AllowNoPassword'] = false;  
cfg['Servers'][$i]['connect_type'] = 'tcp';  
cfg['Servers'][$i]['extension'] = 'mysqli';  
cfg['Servers'][$i]['port'] = '3306';  
cfg['Servers'][$i]['user'] = <име за вход в базата>;  
cfg['Servers'][$i]['password'] = <парола за вход в базата>;
```

примерен endpoint за базата: mydatabase.cuci71cyntah.eu-central-1.rds.amazonaws.com
- Преименувайте файла така, за да се отразят промените
sudo mv config.sample.inc.php config.inc.php
- Рестартирайте сървъра и базата данни
**sudo systemctl restart httpd
sudo systemctl restart mariadb**
- Можете да достъпвате сайта на сървъра си като използвате публичния IP адрес на EC2 инстанцията по този начин
http://<адрес>/<път до файл спрямо главната директория>
Пример: **http://3.120.207.9/web%20project/home.html**



Фигура 23: Достъп до сайта на EC2 с адреса му

- По подобен начин можете да влезете в RНРMyAdmin системата и да управлявате базата от данни на сайта



Фигура 24: Влизане с phpMyAdmin в базата от данни

7 Примерни данни

8 Описание на програмния код

Самият код за сайта е описан в документацията за проекта по Уеб.

9 Приноси на студента, ограничения и възможности за бъдещо развитие

Като бъдещо развитие могат да се интегрират други Amazon сървиси - например такива за защита като AWS WAF, Inspector, GuardDuty. Може да се направи и домейн за сайта и да се контролира трафика с Route 53.

10 Какво научих

Научих как да качвам EC2 инстанция и да се свързвам с нея с Windows PowerShell. Също така разбрах повече за начина, по който работи VPC и за security групите. Научих как да инсталирам пакети от Linux терминала и да конфигурирам файла за RHPMyAdmin, за да имам достъп до базата от данни за сайта и да я управлявам. Запознах се с основната структура на тех документ и команди нужни за оформление на страница и документацията.

11 Списък с фигури

Списък на фигурите

1	Избиране на име и регион за bucket	4
2	Избиране на настройки за енкриптиране на обекти в bucket	4
3	Качване на файлове в създадения bucket	5
4	Избиране на политика за достъп на EC2 до S3 обекти	5
5	Избиране на AMI за EC2	6
6	Избиране на VPC за EC2	6
7	Добавяне на памет EBS към EC2	7
8	Добавяне на правила в security групата на инстанцията	7
9	Създаване на key pair за достъп до EC2	8
10	Стартирана EC2 инстанция с публично IPv4	8
11	Свързване с EC2 в Windows PowerShell	9
12	Избиране на тип база от данни за сървър	10
13	Избиране на версия и име на базата	10
14	Избор на име и парола за вход в базата	11
15	Избор на памет за базата	11
16	Свързване на базата със сървър	12
17	Избиране на VPC и създаване на подмрежова група за базата	12
18	Прикачване на групата към RDS инстанцията	13
19	Избор на автентикация с базата, зона и порт	13
20	XAMPP контролен панел със стартиран сървър	14

21	Стартирана RDS база	14
22	Стартиран EC2	14
23	Достъп до сайта на EC2 с адреса му	16
24	Влизане с phpMyAdmin в базата от данни	16

12 Използвани източници

[1] Host a dynamic website on AWS

[2] Connect AWS RDS MySQL instance with phpMyAdmin

[3] AWS official site