

4.3 - HANDS ON: CRIANDO UM WEBSERVER COM WORDPRESS

Configurando seu banco de dados do RDS

Neste ponto, você já criou um banco de dados do RDS e uma instância do EC2. Neste módulo, vamos configurar o banco de dados do RDS para permitir acesso a entidades específicas.

Métodos de segurança de banco de dados

É crucial proteger seu banco de dados contra acesso não autorizado e há diversas estratégias que você pode usar para deixar seu banco de dados mais seguro. Você aprenderá duas delas neste módulo. Estamos falando de:

- **Segurança de rede:** a limitação do acesso à sua instância de banco de dados mediante a rejeição do tráfego que não é proveniente de endereços IP autorizados.
- **Autorização e autenticação de senha:** a limitação do acesso ao seu banco de dados mediante a solicitação de nome de usuário e senha para o acesso.

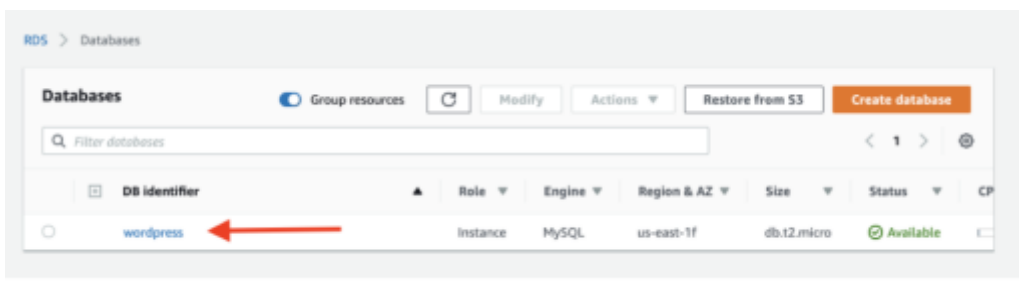
Você vai configurar cada uma dessas nas etapas abaixo.

Etapla 1. Permita que sua instância do EC2 acesse seu banco de dados do RDS

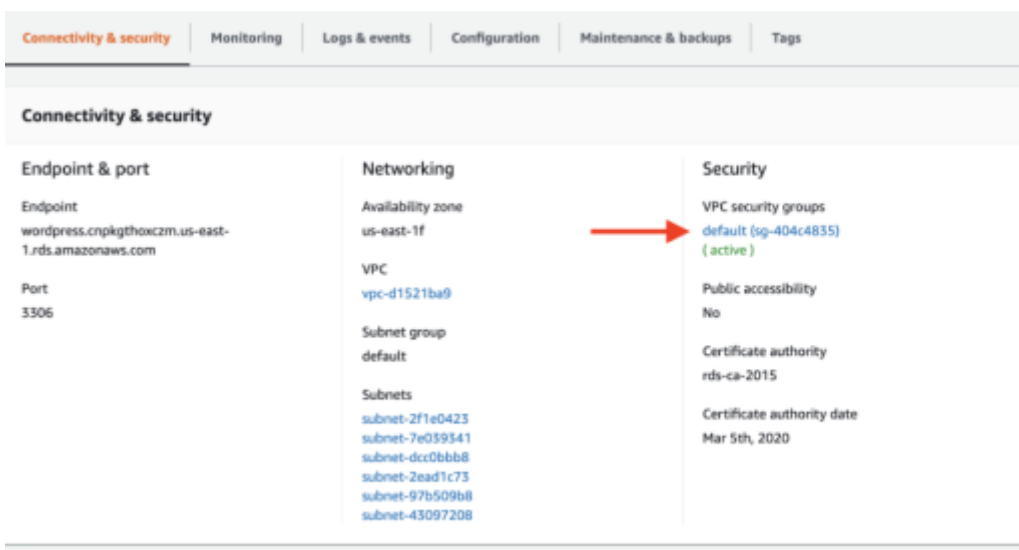
Primeiramente, você modificará seu banco de dados do RDS para permitir o acesso de rede originado em sua instância do EC2.

No módulo anterior, você criou regras de grupo de segurança para permitir tráfego SSH e HTTP para sua instância do EC2 do WordPress. O mesmo princípio é aplicado aqui. Desta vez, você deseja permitir o tráfego específico de sua instância do EC2 para seu banco de dados do RDS.

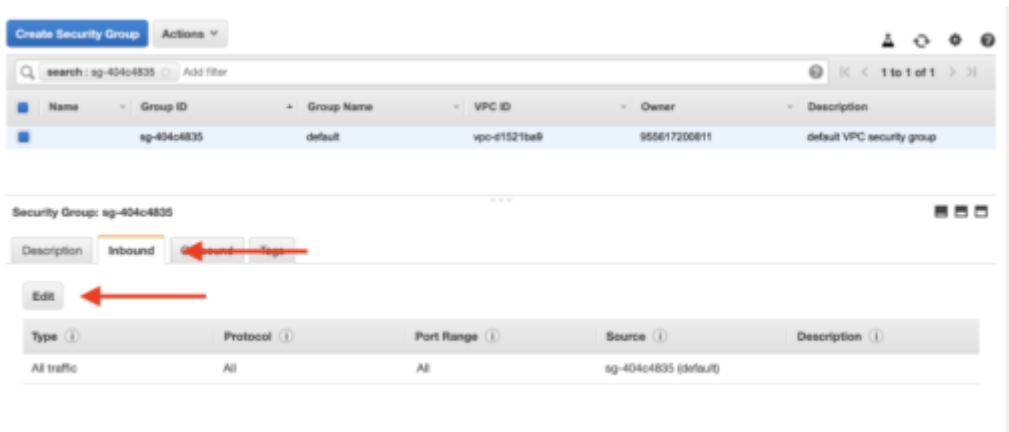
Para configurar isso, acesse o [RDS](#) no Console AWS. Clique no banco de dados MySQL que você criou em um módulo anterior neste laboratório.



Role até a guia **Connectivity & security** (Conectividade e segurança) na página exibida e clique no grupo de segurança listado em **VPC security groups** (Grupos de segurança de VPC).



O console vai levá-lo ao grupo de segurança configurado para seu banco de dados. Clique na guia **Inbound** (Entrada), e então no botão **Edit** (Editar) para alterar as regras de seu grupo de segurança.



O grupo de segurança padrão tem uma regra que permite todo o tráfego recebido de outras instâncias que estão no grupo de segurança padrão. No entanto, como sua instância do EC2 do WordPress não está nesse grupo de segurança, ela não terá acesso ao banco de dados do RDS.

Altere a propriedade **Type** (Tipo) para **MYSQL/Aurora**, o que vai atualizar o **Protocol** (Protocolo) e o **Port Range** (Intervalo de portas) para os valores adequados.



Em seguida, remova o valor do grupo de segurança atual configurado para a regra e digite “wordpress”. O console vai exibir os grupos de segurança disponíveis que estão configurados.

Edit inbound rules

Type	Protocol	Port Range	Source	Description
MySQL/Aurora	TCP	3306	Custom sg-604c4835	e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

Clique no grupo de segurança “wordpress” que você usou para sua instância do EC2.

Edit inbound rules

Type	Protocol	Port Range	Source	Description
MySQL/Aurora	TCP	3306	Custom word	e.g. SSH for Admin Desktop

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

Após seu clique, ele será preenchido no ID do grupo de segurança. Essa regra permitirá o acesso ao MySQL para qualquer instância do EC2 configurada com esse grupo de segurança.

Após concluir, clique no botão azul **Save** (Salvar) para salvar as alterações.

Edit inbound rules

Type	Protocol	Port Range	Source	Description
MySQL/Aurora	TCP	3306	Custom sg-0e1138bb2aa60a3fd	e.g. SSH for Admin Desktop

Add Rule

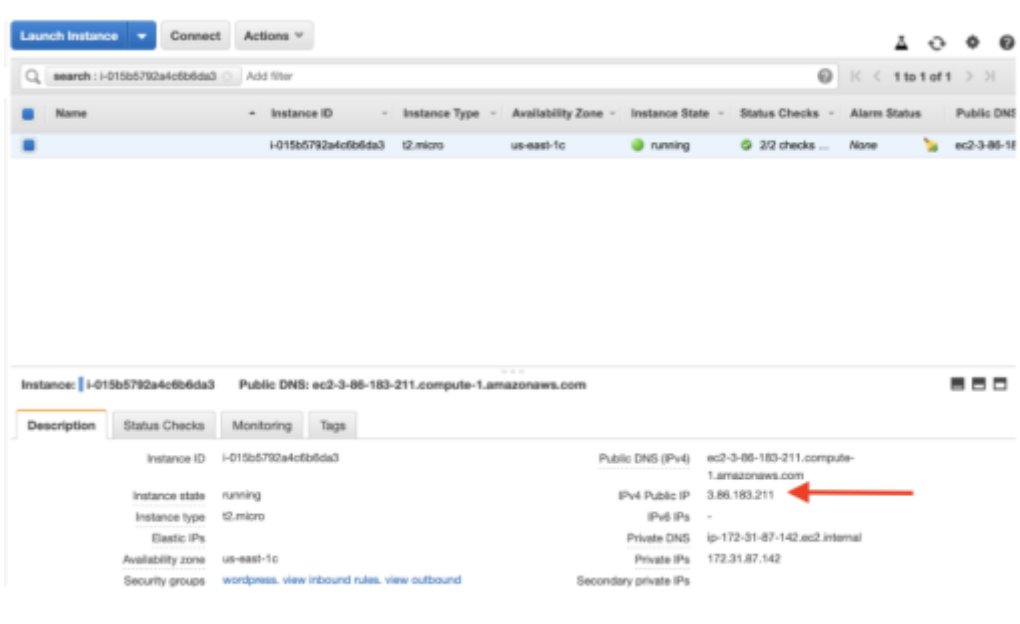
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Save

Etapa 2. Conecte-se à sua instância do EC2 usando SSH

Agora que sua instância do EC2 tem acesso ao seu banco de dados do RDS, você vai se conectar à sua instância do EC2 usando SSH e executar alguns comandos de configuração.

Acesse a [página de instâncias do EC2](#) no Console AWS. Você deve ver a instância do EC2 que criou para a instalação do WordPress. Clique nela e você verá um endereço IP público com o rótulo **IPv4 Public IP** (IP público Ipv4) na descrição da instância.



Salve esse endereço IP, pois você precisará dele ao conectar-se por SSH em sua instância.

Anteriormente, você fez download do arquivo .pem para o par de chaves de sua instância. Localize esse arquivo agora. Provavelmente ele estará em uma pasta de **Downloads** ou em sua área de trabalho.

Para usuários de Mac ou Linux:

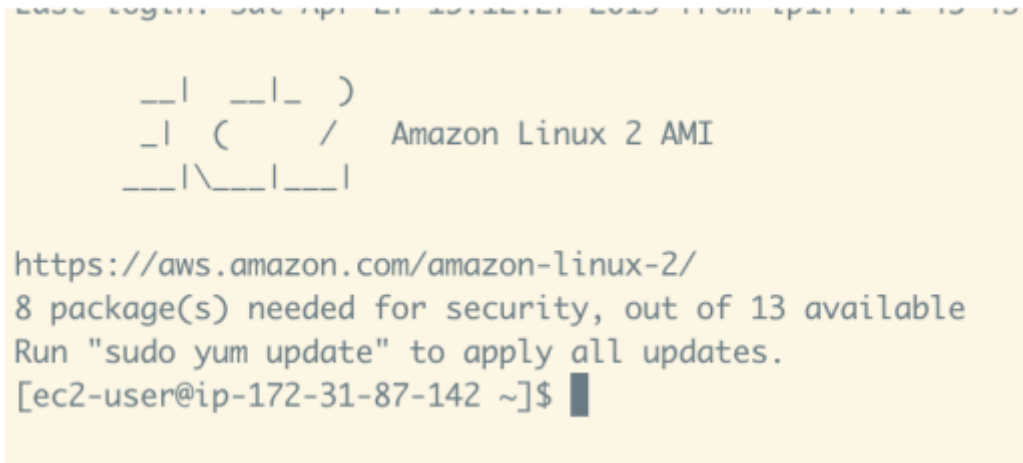
Abra uma janela do terminal. Caso esteja em um Mac, é possível usar o programa **Terminal** padrão que está instalado ou ainda usar o seu próprio terminal.

Em seu terminal, execute os seguintes comandos para estabelecer a conexão à sua instância usando SSH. Substitua o “<path/to/pem/file>” com o caminho para seu arquivo, p. ex., “~/Downloads/wordpress.pem”, e o “<publicIpAddress>” com o endereço IP público para sua instância do EC2.

```
chmod 600 <path/to/pem/file>
```

```
ssh -i <path/to/pem/file> ec2-user@<publicIpAddress>
```

Você deve ver o seguinte resultado em seu terminal para indicar o êxito da conexão:

A screenshot of a terminal window with a yellow background. It shows the output of an SSH command. At the top, there is a decorative ASCII art logo consisting of several lines of underscores and parentheses. Below the logo, the text "Amazon Linux 2 AMI" is displayed. Further down, the terminal shows the URL "https://aws.amazon.com/amazon-linux-2/", followed by the message "8 package(s) needed for security, out of 13 available" and "Run 'sudo yum update' to apply all updates." The prompt "[ec2-user@ip-172-31-87-142 ~]\$" is visible at the bottom, with a black cursor block following the dollar sign.

```
__|  __|_ )  
_| (    /  Amazon Linux 2 AMI  
__|\___|___|  
  
https://aws.amazon.com/amazon-linux-2/  
8 package(s) needed for security, out of 13 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-87-142 ~]$ █
```

Para usuários do Windows:

Para estabelecer conexão com sua instância do EC2, será necessário usar o [PuTTY](#), um cliente SSH para Windows. Para obter instruções sobre como fazer isso, consulte o guia [Conectar-se à sua instância do Linux no Windows usando PuTTY](#). Você vai precisar do arquivo .pem que baixou e do endereço IP público de sua instância do EC2.

Nesta etapa, você se conectou à sua instância do EC2 por SSH. Na próxima etapa, você vai se conectar ao seu banco de dados do RDS diretamente de sua instância do EC2 e criar um usuário de banco de dados para o aplicativo WordPress.

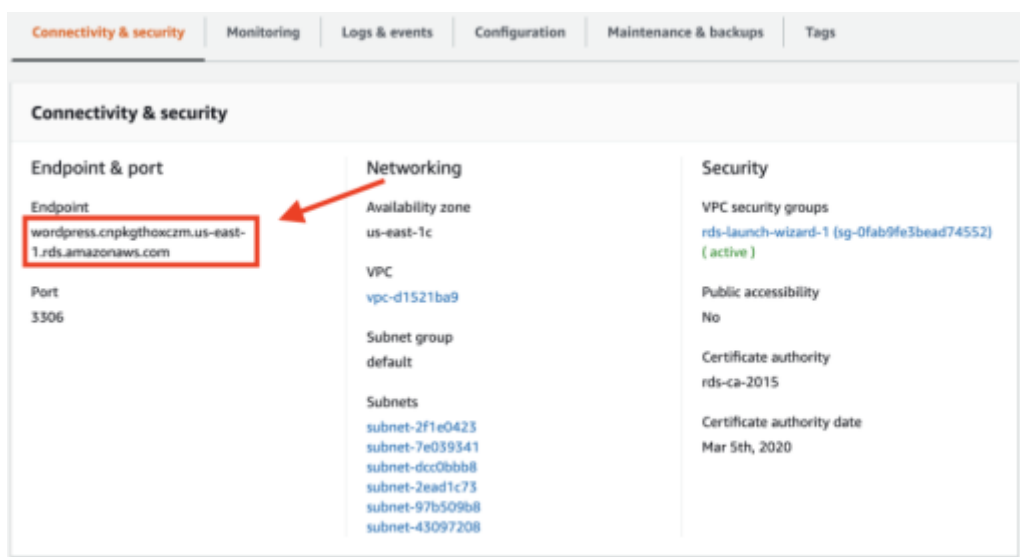
Etapa 3. Criando um usuário de banco de dados

Você deve ter uma sessão SSH para sua instância do EC2 ativa no terminal. Agora, você vai se conectar ao seu banco de dados MySQL.

Primeiramente, execute o seguinte comando em seu terminal para instalar um cliente MySQL para interagir com o banco de dados.

```
sudo yum install -y mysql
```

Em seguida, localize o nome do host de seu banco de dados do RDS no Console AWS. Nos detalhes de seu banco de dados do RDS, o nome do host será exibido como o **Endpoint** na seção **Connectivity & security** (Conectividade e segurança).



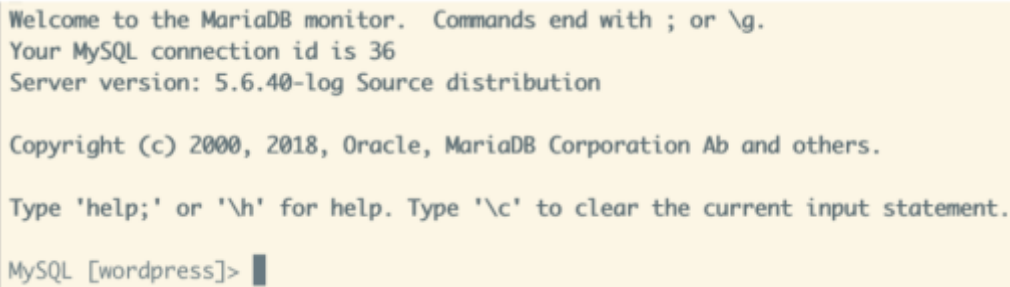
Em seu terminal, insira o seguinte comando para definir uma variável de ambiente para seu host MySQL. Não esqueça de substituir “<your-endpoint>” pelo nome do host de sua instância do RDS.

```
export MYSQL_HOST=<your-endpoint>
```

Em seguida, execute o seguinte comando em seu terminal para estabelecer a conexão com seu banco de dados MySQL. Substitua “<user>” e “<password>” pelo nome de usuário mestre e senha configurados ao criar seu banco de dados do RDS.

```
mysql --user=<user> --password=<password> wordpress
```

Caso a conexão tenha sido estabelecida com êxito, seu terminal deve indicar a conexão com o banco de dados MySQL conforme exibido na imagem a seguir.

A screenshot of a terminal window with a yellow background. It displays the output of a MySQL connection command. The text reads: 'Welcome to the MariaDB monitor. Commands end with ; or \g. Your MySQL connection id is 36 Server version: 5.6.40-log Source distribution Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. MySQL [wordpress]>'.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.6.40-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [wordpress]> █
```

Por fim, crie um usuário de banco de dados para seu aplicativo WordPress e conceda permissão para ele acessar o banco de dados “wordpress”.

Execute o seguinte comando em seu terminal:

```
CREATE USER 'wordpress' IDENTIFIED BY 'wordpress-pass';

GRANT ALL PRIVILEGES ON wordpress.* TO wordpress;

FLUSH PRIVILEGES;

Exit
```

Você deve usar uma senha melhor que “wordpress-pass” para proteger seu banco de dados.

Anote tanto o nome de usuário quanto a senha configurados, pois você precisará deles no próximo módulo durante a configuração de sua instalação do WordPress.

Neste módulo, você aprendeu como configurar a segurança de rede e com senha para seu banco de dados do RDS. Agora sua instância do EC2 tem acesso de rede ao seu banco de dados do RDS. Além disso, você criou um usuário de banco de dados que será usado por seu aplicativo WordPress.

No próximo módulo, você vai configurar sua instância do EC2 para executar o aplicativo WordPress.