

4.2 - HANDS ON: CRIANDO UM WEBSERVER COM WORDPRESS

Criação de uma instância do EC2

Neste módulo, você criará uma instância do Amazon EC2 para executar seu site do WordPress. O Amazon EC2 oferece instâncias de servidor altamente configuráveis sob demanda. Em uma instância do EC2, você pode executar o site do WordPress que ficará acessível para os usuários em qualquer lugar.

Por que usar o Amazon EC2 para seu site do WordPress

Ao começar com o WordPress, você pode testá-lo instalando e executando-o no seu laptop ou desktop. Ele funciona bem para um teste, mas você logo atingirá as limitações. Seu site do WordPress só estará em execução enquanto seu laptop ou desktop estiver em execução. Além disso, o site só ficará acessível para você -- ele não ficará disponível publicamente na internet.

Uma melhor abordagem é usar um *servidor*.

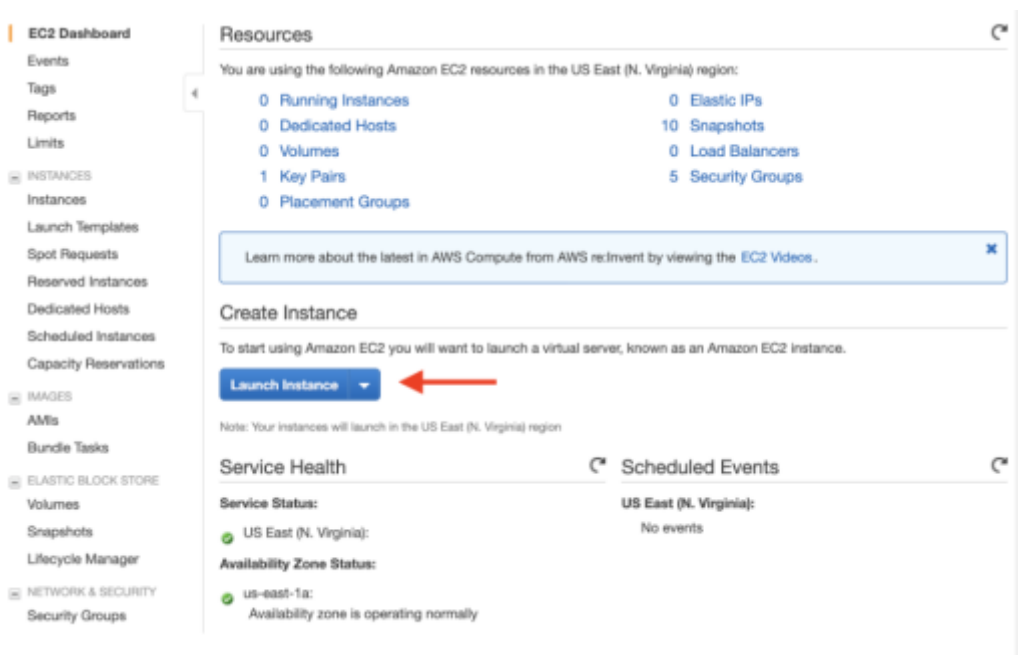
O Amazon EC2 fornece provisionamento de servidor sob demanda. Com o Amazon EC2, você aluga instâncias de servidor com tamanhos variados, cada uma com diferentes configurações de CPU, RAM e rede. Você paga por hora por esses servidores e pode usá-los para hospedar sites, como o seu site do WordPress. Com uma instância do EC2, seu site WordPress permanecerá em funcionamento e estará acessível por qualquer pessoa pela Internet.

Nas etapas abaixo, executaremos um instância do EC2 para hospedar seu site do WordPress.

Etapas 1. Seleção de uma Amazon Machine Image

Para criar sua instância do EC2, acesse [Amazon EC2 no console AWS](#). Clique no botão azul **Executar instância** para abrir o assistente de criação de instância.

Na primeira página, você escolherá uma Amazon Machine Image (“AMI”). A AMI que você escolher determinará o software de base que está instalado na sua nova instância do EC2. Isso inclui o sistema operacional (Amazon Linux, Red Hat Enterprise Linux, Ubuntu, Microsoft Server etc.), assim como os aplicativos que estão instalados na máquina.



Diversas AMIs são AMIs de uso geral para executar muitos aplicativos diferentes, mas algumas são criadas especificamente para casos de uso específicos, como a AMI do Deep Learning ou várias AMIs do AWS Marketplace.

O Amazon Linux distro é uma escolha bem conhecida, então selecione a AMI do Amazon Linux 2 (HVM) na exibição de seleção da AMI.

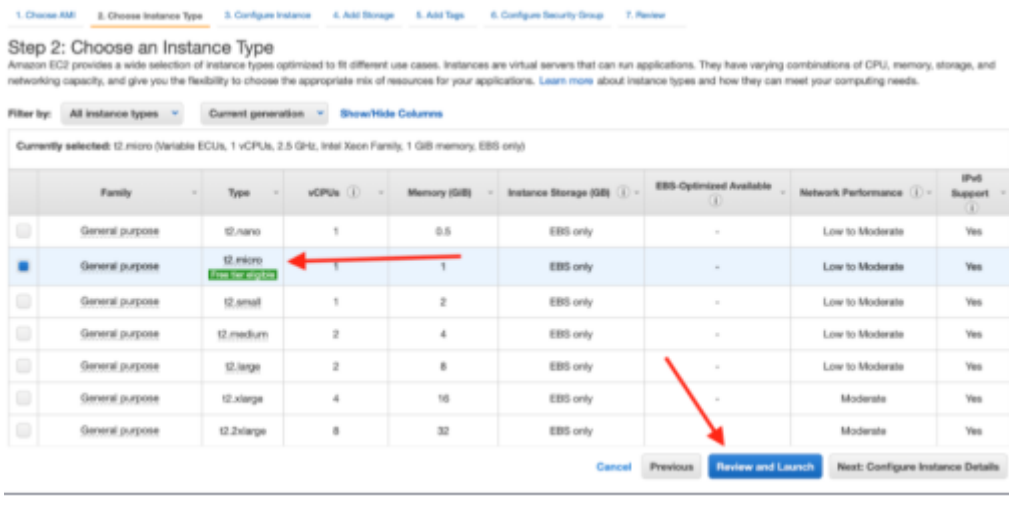


Etapa 2. Escolher um tipo de instância

Na segunda tela do assistente do EC2, você selecionará um tipo de instância do EC2. Um tipo de instância é uma configuração particular de CPU, memória (RAM), armazenamento e capacidade de rede.

A AWS tem uma grande seleção de tipos de instâncias que abrange muitas cargas de trabalho diferentes. Algumas são direcionadas a cargas de trabalho com muita memória, como banco de dados e armazenamento em cache, outras focam cargas de trabalho com computação intensa, como processamento de imagens e codificação de vídeo.

O Amazon EC2 permite que você execute 750 horas por mês de uma microinstância t2.no nível gratuito da AWS. Selecione esta opção para este laboratório. Desse modo, você não terá qualquer custo na sua fatura.



Depois de selecionar a microinstância t2, clique no botão azul **Analisar e executar** para ignorar algumas etapas da configuração avançada.

Etapa 3. Configuração de grupos de segurança

Depois de clicar no botão **Analisar e executar**, você será levado para uma tela de Análise de execução de instância. Você precisa configurar mais uma coisa antes de executar sua instância.

Os grupos de segurança são regras de rede que descrevem o tipo de tráfego de rede permitido em sua instância do EC2. Você deseja permitir dois tipos de tráfego em sua instância:

- Tráfego **SSH** do seu endereço IP atual, para que você possa usar o protocolo SSH para fazer login na instância do EC2 e configurar o WordPress;
- Tráfego **HTTP** de todos os endereços IP para que os usuários possam visualizar seu site do WordPress.

Para configurar isso, clique no link **Editar grupos de segurança** na página de análise.

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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0de53d6696e8dcf90

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 215, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Next Device Type: x86_64 Next Substitution type: none

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1
Description: launch-wizard-1 created 2019-04-27T09:32:34.735-05:00

Type	Protocol	Port Range	Source	Description
This security group has no rules.				

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

Ele mostrará as regras atuais no seu grupo de segurança.

Há uma regra de SSH configurada, mas ela permite o acesso do SSH de qualquer endereço IP. Clique em **Fonte** para restringi-la ao seu endereço IP atual.

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: launch-wizard-1
Description: launch-wizard-1 created 2019-04-27T09:32:34.548-05:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	✓ Custom Anywhere 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning

Em seguida, você precisará adicionar uma nova regra para permitir o tráfego de HTTP. Clique em **Adicionar regra**.

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: launch-wizard-1

Description: launch-wizard-1 created 2019-04-27T09:32:34.548-05:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 174.71.45.43/32	e.g. SSH for Admin Desktop

Add Rule

Na regra nova que aparece, clique na lista suspensa na coluna **Tipo**. Selecione **HTTP** e os valores padrão para uma regra de HTTP serão preenchidos automaticamente.

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 174.71.45.43/32	e.g. SSH for Admin Desktop
Custom TCP	TCP		Custom CIDR, IP or Security Group	e.g. SSH for Admin Desktop

Add Rule

Depois de por as regras do grupo de segurança em funcionamento, dê um nome ao seu grupo de segurança na caixa de entrada **Nome do grupo de segurança**. Dê o nome de “wordpress” ao grupo para que ele seja fácil de localizar.

Depois de dar o nome ao grupo, clique no botão azul **Analisar e executar**.

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: wordpress

Description: Wordpress Security Group

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 174.71.45.43/32	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

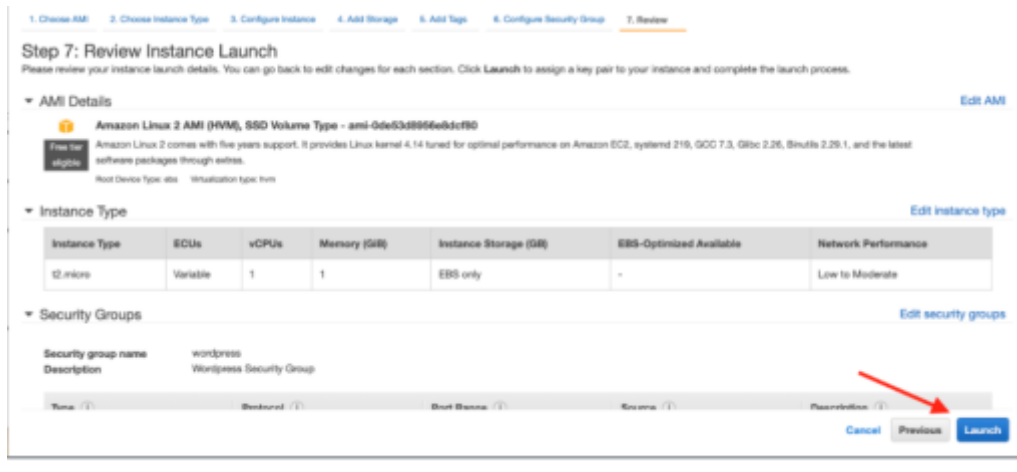
Add Rule

Cancel

Review and Launch

Etapa 4. Executar e obter um chave SSH

Agora é hora de executar sua instância do EC2. Clique no botão azul **Executar** para criar sua instância do EC2.



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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0de53d8856e8dcf90

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Strutils 2.25.1, and the latest software packages through extras.

Root Device Type: xbs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name	Description
wordpress	WordPress Security Group

Cancel Previous **Launch**

Você verá detalhes sobre como configurar um par de chaves para a sua instância. Você usará o par de chaves para executar o SSH em sua instância, que dará a você a habilidade de executar comandos no seu servidor.

Crie um novo par de chaves para sua instância e dê a ele um nome. Em seguida, clique no botão **(Fazer download do par de chaves)** para baixar o arquivo .pem em sua máquina, que você usará no próximo módulo.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

wordpress

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

Depois de ter feito o download do seu par de chaves, clique no botão azul **Executar instâncias** para executar a sua instância do EC2.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

wordpress

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

Você executou com êxito a sua instância do EC2. No próximo módulo, você configurará o seu banco de dados do RDS para operar com a sua instância do EC2.