

06

Mão à obra: Criando configuração personalizada

Agora que temos a imagem customizada, devemos estabelecer o vínculo e informar aos demais servidores do grupo de auto-escalonamento que irão utilizá-la. O primeiro passo é ir até o painel de console da Amazon e procurar pelo serviço EC2, feito isso, no painel lateral esquerdo, abaixo da aba Auto Scaling clique na opção Launch Configuration para que possamos criar essa configuração personalizada que será utilizada pelos demais servidores.



Posteriormente, clique no botão Create Launch Configuration. Devemos fazer a configuração que os demais servidores do grupo terão. O primeiro passo é escolher qual imagem deverá ser utilizada pelos demais servidores, vá até a opção My AMIs e escolha a opção da imagem que criamos na etapa anterior imagem-casadocodigo.

Create Launch Configuration

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start Cancel and Exit

My AMIs Search my AMIs

AWS Marketplace 1 to 1 of 1 AMIs

Community AMIs Select

Ownership 64-bit

imagem-casadocodigo - ami-efcaeae95
Root device type: ebs Virtualization type: hvm Owner: 1341844858

Feito isso, na próxima tela de configuração, devemos ter as configurações das máquinas utilizadas para as demais instâncias que farão parte do grupo, por padrão a Amazon irá configurar a máquina **t2.micro** de uso gratuito, mantenha essa configuração e clique em **Next**. Na próxima etapa, dê o nome para essa configuração customizada que estamos fazendo como sendo **imagem-customizada-casadocodigo**. Clique na opção **Advanced Details** e peça para a Amazon fornecer um endereço IP público para essas instâncias que farão parte do grupo, **Assign a public IP address to every instance**, para que possamos fazer diretamente o acesso delas pela internet, para comprovar que de fato o escalonamento foi realizado com sucesso.

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

Create Launch Configuration

Advanced Details

Kernel ID: Use default

RAM Disk ID: Use default

User data: As text (Optional)

IP Address Type: Assign a public IP address to every instance (selected)

Note: this option only affects instances launched into an Amazon VPC

Seguindo na configuração devemos informar o grupo de segurança que deverá ser associado as demais instâncias que farão parte do grupo de auto-escalonamento. No caso, nós já havíamos criado o grupo de segurança chamado **SG-EC2** liberando a porta 22 para o protocolo SSH bem como a porta 8080 utilizada pelo Tomcat, podemos utilizar esse mesmo grupo para ser utilizado pelas demais instâncias que farão parte do grupo de auto-escalonamento.

Create Launch Configuration

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 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 Learn more about Amazon EC2 security groups.

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

Security Group ID	Name	VPC ID	Description
<input type="checkbox"/> sg-a04058d2	default	vpc-3e59e246	default VPC security group
<input type="checkbox"/> sg-0e950a7b	rds-launch-wizard-2	vpc-3e59e246	Created from the RDS Management Console
<input checked="" type="checkbox"/> sg-634bd116	SG-EC2	vpc-3e59e246	launch-wizard-1 created 2017-12-01T10:32:13.368-02:00

Para finalizar clique no botão **Create launch configuration** e informe que iremos acessar os demais servidores do grupo com a mesma chave que fizemos o download na etapa anterior **chave_EC2_1.pem**

Select an existing key pair or create a new key pair X

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](#).

Choose an existing key pair ▼

Select a key pair chave_EC2_1 ▼

I acknowledge that I have access to the selected private key file (chave_EC2_1.pem), and that without this file, I won't be able to log into my instance.

Create launch configuration Cancel

Feito isso, iremos na próxima etapa criar as políticas de auto-escalonamento para que tenhamos os demais servidores utilizando essas configurações que fizemos agora.