CURSO AWS

Primeiro devemos abrir uma conta na AWS.

Ir em serviço e digita IAM.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Autenticacao com o Microsoft Authenticator

Ir em usuários e criar uma conta

CLI – que é a interface pela linha de comando ou pelo dashboard

O Amazon **Lightsail** é um provedor de servidor privado virtual (VPS) e a maneira mais fácil de começar a usar a **AWS** para desenvolvedores, pequenas empresas, estudantes e outros usuários que precisam de uma solução para construir e hospedar suas aplicações na nuvem.

Vamos criar a instancia

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Cria tudo em default

IP ESTATICO E DNS PARA O WORDPRESS

Aqui esta o ip da nossa instancia

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente



Se pegarmos este IP e colocarmos no browser ele vai aparecer a sua aplicação. Se no final do IP digitar /wp-admin ele vai aparecer o usuário e senha para mexermos na instancia.

Onde esta circulado na figura acima, se clicar nele ele vai abrir um console, nele vamos digitar conforme na figura abaixo.

Texto

Descrição gerada automaticamente

Notar que o usuário e senha já estão aparecendo no console, vamos pegar ela colar onde abrir o wordpress. A instancia já esta no ar.

Se vc for colocar em produção é interessante que o IP seja estático, para isso vamos acessar o gerenciamento da instancia clicando nos 3 pontos

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Vamos na aba Networking, vamos criar um IP estático. Vamos deixar tudo como paDRAO E CRIAR. Fazendo isso já deixamos em produção.

Para não deixarmos o IP a mostra, vamos criar um domínio, para isso vamos criar um bem barato conforme mostra na figura abaixo

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

**AMAZON EC2: ALTA DISPONIBILIDADE E ESCALABILIDADE EM UMA APLICAÇÃO**

EC2 (Elastic Computing Cloud) é um serviço de criação de servidores virtuais da amazon.

Primeiramente vamos criar uma instancia. Vamos dar um nome para ela, por exemplo ec2-first.

Depois vamos selecionar uma imagem, neste caso vamos utilizar Amazon Linux. Em seguida vamos escolher o tipo de instancia, sempre se atentarse a instancia criada esta de acordo com a região que foi selecionada.

Vamos precisar ter um par de chaves para garantir que conseguimos acessar sem precisar ficar colocando senha. Vamos criar um par de chaves, neste cas RSA e o formato.pem. Vamos salvar este arquivo dentro de alguma pasta e depois vamos colocar o arquivo dentro da pasta .ssh.

Para a chave ficar mais segura, vamos diminuir a quantidade de permissão e para isso vamos utilizar o comando chmod que é um comando de modificar permissões e colocar 400 que é um numero que o Linux utiliza que só vai permitir a leitura dessa chave somente para o seu usuário.

Em configurações de redes vamos manter o padrão.

Toda instancia ou maquina que será criada, precisamos ter um HD o que será configurado em configurar armazenamento.

Feito isso vamos executar a maquina.

Ao clicar no ID da instancia, vai aparecer varias informações em relação a instancia. Uma delas é o conectar onde vamos copiar o comando que se encontra no cliente ssh. Este comando será colado no terminal ssh -i “ec2.pem” o numero do comando copiado. Ao clicar em enter, automaticamente ele vai adicionar este IP a esta nova maquina.

**SECURITY GROUPS**

Assim que criamos uma instancia, automaticamente ele cria um grupo de segurança por Default.

Ao clicar no default ele vai ter as regras de entrada e de saída no qual todo o trafego esta liberado.

Por padrão, já é criado o grupo launch-wizard-1. Este grupo possui uma regra um pouco diferente, no qual ele libera a entrada utilizando o SSH no qual podemos alterar isso para não permitir o acesso de todo mundo. Para isso vamos em editar regra e modifica-la colocando a origem como MEU IP, no qual a amazon vai identificar o ip publica da sua maquina e somente ele será utilizado.

Não há necessidade de ter um security group para cada instancia. Para isso vamos em criar um grupo de segurança. Na regra de entrada, vamos configurar o tipo HTTP e na origem vamos selecionar o IPv4 e IPv6 , para isso vamos selecionar “Personalisado” e digitar o IP 0.0.0.0/0.::/0.

Vamos configurar o HTTPS vamos selecionar “Personalisado” e digitar o IP 0.0.0.0/0.::/0.

Para a saída não vamos configurar nada pois vamos permitir qualquer saída.

Vamos voltar nas instancias, ir em ações, segurança onde vamos alterar o grupo de segurança.

Security groups controlam o acesso a rede da instância, sendo assim, podemos bloquear ou liberar tráfego, assim como fazemos com firewalls.

**Opinião do instrutor**

1. Logado em sua conta no console AWS, acesse o serviço EC2;
2. Na sessão “Instâncias”, clique no botão “Executar instâncias” para criar uma nova instância EC2;
3. Defina um nome para sua instância e selecione a imagem padrão (Amazon Linux);
4. Deixe todas as opções padrão até chegar em “Par de chaves (login)”;
5. Crie um novo par de chaves. Mantenha as opções padrão e faça o download da sua chave;
6. Altere as permissões de sua chave com chmod 400 sua-chave.pem;
7. Finalize clicando em “Executar instância”;
8. Com a instância sendo executada, acesse os detalhes da instância e vá até “Conectar”. Siga as instruções para se conectar à instância;
9. Vá até “Security group” e edite as regras de entrada do security group criado para nossa instância, permitindo acesso somente de “Meu IP”;
10. Crie um novo Security group para liberar acesso web (portas 80 e 443);
11. Vá até “Instâncias” e adicione esse Security group à instância criada anteriormente.

Uma região geralmente recebe o nome da cidade onde se encontra. São Paulo, por exemplo, é uma região da AWS no momento da gravação desse treinamento. E dentro dessa região, há 3 espaços físicos que possuem sub-redes conectadas entre si. Estes espaços físicos são chamados de zonas de disponibilidade. Cada zona de disponibilidade pode ser uma sala, um andar ou até um prédio diferente dentro da região em questão.

1. Encerre a instância criada no capítulo anterior;
2. Crie uma nova instância e na sessão de imagem, clique em “Procurar mais AMIs” para selecionar uma imagem diferente;
3. Em “AMIs do AWS Marketplace” procure por “nginx” e selecione a imagem gratuita chamada “NGINX Open Source packaged by Bitnami”;
4. Continue a criação da instância normalmente, atrelando a ela os grupos de segurança já criados;
5. Dê um nome (algo como “nginx”) para a instância recém criada;
6. Nos detalhes da instância, clique para acessar o endereço de DNS público dessa instância. Na aba aberta, substitua “https” por “http”. A página de boas-vindas da imagem deve ser exibida com sucesso;
7. Se conecte, via ssh, à instância usando o usuário “bitnami”.

CRIANDO UMA IMAGEM

Ao criarmos uma instância a partir de uma imagem, podemos selecionar todo o hardware (tipo de instância, rede, etc) e algum software já vem pré-instalado. No exemplo da aula foi o Nginx. Já com o Modelo, nós podemos selecionar qualquer imagem e o hardware já estará pré-configurado. Inclusive nós criaremos um modelo mais adiante no curso para que a AWS possa criar instâncias automaticamente para nós.

Esta é a condição para que você tenha o Elastic IP de forma gratuita. Caso haja mais IPs anexados a uma instância ou a instância seja desligada, você será cobrado.

1. Selecione a instância “nginx” e crie uma imagem a partir dela;
2. Após a imagem ficar disponível, execute uma nova instância a partir dessa imagem;
3. Após as verificações de status finalizarem, acesse a instância para confirmar que tudo funcionou como esperado;
4. Encerre essa última instância para evitar custos, já que não vamos mais utilizá-la;
5. Reinicie a instância “nginx” e veja que seu IP e seu DNS vão mudar;
6. Acesse a página de “IPs elásticos” e aloque um novo IP com todas as opções padrão;
7. Clique no IP recém criado e o associe à instância “nginx”;
8. Acesse [http://seu-ip-elastico](http://seu-ip-elastico/) para conferir que o acesso à instância está ocorrendo com sucesso;
9. Entre na instância (via ssh) e execute sudo apt update && sudo apt install posgresql para instalar o PostgreSQL na instância;
10. Na busca do console da AWS, pesquise por RDS e acesse o painel desse serviço;
11. Crie um novo banco de dados compatível com PostgreSQL no Nível gratuito;
12. Veja os detalhes de conexão para copiar sua senha. Copie também o endpoint (host) do banco;
13. Adicione à sua instância o security group “default” que permite todo tráfego dentro da VPC;
14. Quando o banco estiver disponível, acesse novamente (via ssh) sua instância EC2 e se conecte ao banco através do comando psql -U postgres -p -h seu-endpoint-rds-aqui e após digitar “Enter”, entre com sua senha.

Loading Balance

1. Selecione a instância “nginx” e a duplique através da opção “Executar mais como essa”. Crie essa nova instância em outra zona de disponibilidade e chame-a de “nginx-2";
2. Em “Load balancers” crie um novo “Application Load Balancer” nas zonas de disponibilidade de suas 2 instâncias;
3. Adicione a esse load balancer o grupo de segurança “acesso-web” para que ele seja acessível via HTTP;
4. Na parte de roteamento do load balancer, crie um novo target group com as 2 instâncias e selecione esse target group como ação do load balancer;
5. Com o load balancer criado e ativo, acesse o DNS dele para garantir que tudo está funcionando;
6. Edite o HTML em /opt/bitnami/nginx/html/index.html em suas duas instâncias com conteúdos diferentes para podermos diferenciá-las;
7. Após editar e salvar, acesse o endereço do load balancer de novo e ao atualizar a página várias vezes você deve ver o conteúdo sendo alternado, mostrando que cada requisição chega em uma instância diferente;
8. Desligue uma das instâncias e veja que o load balancer continua acessível, mandando todo o tráfego para a instância que está de pé;
9. Caso você possua um domínio, crie uma entrada do tipo CNAME apontando para o DNS do load balancer e após a propagação, acesse através desta entrada;
10. Crie um novo grupo de auto scaling usando um modelo de execução. Crie esse modelo com a imagem que criamos anteriormente e as configurações de hardware que já estamos habituados;
11. Selecione quais zonas de disponibilidade serão utilizadas por esse grupo de auto scaling (lembre-se de utilizar as mesmas que selecionou no load balancer, senão o load balancer não conseguirá redirecionar o tráfego);
12. Anexe esse grupo de auto scaling ao nosso balanceador de carga existente;
13. Com o grupo criado, modifique a capacidade desejada e mínima para 2 e máxima para 3;
14. Remova do target group as 2 instâncias que adicionamos manualmente anteriormente. Também encerre essas instâncias já que não serão mais utilizadas;
15. Em nosso grupo de auto scaling, na aba de escalabilidade automática, define uma plítica de escalabilidade dinâmica para criar mais instâncias quando o uso de CPU passar de 10%.
16. No console da AWS, busque por IAM. Neste serviço, crie um novo usuário com chave de acesso e dê a ele permissões de admin;
17. Instale a AWS CLI em seu sistema operacional seguindo o passo a passo exposto da documentação;
18. Execute o comando aws configure para configurar o acesso da CLI à sua conta;
19. Cole a chave de acesso e depois a chave secreta. Ambas chaves são disponibilizadas no momento da criação do usuário (etapa 1). Deixe as demais opções como padrão;
20. Execute aws ec2 describe-instances --query="Reservations[\*].Instances" --filters="Name=instance-state-name,Values=running" para ver a lista de todas as instâncias que estão executando;
21. Interrompa uma das instâncias com aws ec2 stop-instances --intance-ids {id da instância}. Confira que a instância está interrompida parada e que outra será criada pelo auto scaling group.