
CLOUD
COMPUTING

6

Serviços de Segurança

Prof. Me. Rodolfo Riyoei Goya

Resumo

Na "Computação em Nuvem", particularmente em nuvem pública, os componentes de infraestrutura de rede de Tecnologia da Informação (T.I.) estão em datacenters conectados na Internet e são acessados remotamente. Esta situação os deixa expostos e torna a segurança de rede, seus componentes (como grupos de segurança) e serviços (como listas de acesso) itens prioritários. Abordam-se aqui, como estes conceitos listados são realizados nas implementações reais de nuvens através de exemplos na nuvem da AWS.

6.1. Introdução

Quando se trata de segurança na nuvem, quais são os entes básicos que a compõem? Na "Computação em Nuvem", serviços de lista de acesso e firewall também são virtuais. Como proteger serviços em execução em máquinas virtuais na "Nuvem"? Como filtrar o tráfego que passa de uma sub-rede para outra permitindo apenas o desejado? Como proteger instâncias contra tráfego malicioso?

6.1.1. "Security principals"

Na AWS a segurança é organizada sobre quatro conceitos:

a. "Security principals"
b. Ações/Operações
c. Recurso
d. Políticas

Os "Security principals" são os atores aos quais são permitidas as Ações ou Operações sobre os Recursos. Na AWS, os "Security principals" são: Usuários, Grupos e Aplicações.

Na AWS, as Ações permitem ("Allow") ou negam ("Deny") acesso ao recurso ao passo que a especificação de Operações permite um controle mais fino do que é

permitido ou negado (tais como ler, modificar ou listar objetos: GetObject, PutObject ou ListObject).

Os recursos, na AWS, podem ser especificados no todo, por exemplo todo o serviço de armazenamento do Usuário, ou com controle mais fino, por exemplo, por pasta (ou por Bucket em um S3) ou tipo de arquivo (como foto*.jpg).

As políticas, na AWS, são documentos especificando a relação entre "Security principals" e as Ações/Operações que eles podem executar sobre cada recurso, com um default que nega qualquer Ação/Operação para qualquer "Security principal" sobre qualquer recurso que não seja explicitamente declarada.

6.2. Grupos de Segurança

Para gerenciar o tráfego que entra e sai de instância, a AWS permite criar os Grupos de Segurança. Um grupo de segurança é um conjunto de regras. Cada regra define um tipo de tráfego ("Ação/Operação") que pode ser enviado ou recebido ("Allow").

As instâncias podem ser configuradas para aplicarem um grupo de segurança. Quando isto ocorre, ela obedece às restrições descritas por este grupo.

Diversas instâncias, de uma mesma VPC, podem aplicar o mesmo grupo de segurança e terem, assim, o mesmo perfil de segurança. Um grupo de segurança funciona como um "Firewall" virtual afetando, inclusive, o tráfego entre instâncias que estão dentro de uma mesma sub-rede. Contudo, o grupo de segurança opera como se fosse uma configuração da instância: não há nenhuma máquina virtual dedicada para executar este serviço.

6.2.1. Criação de grupo de segurança

Para criar um grupo de segurança na AWS, a partir da tela inicial do console, deve-se procurar pelo console do EC2.

De lá deve-se selecionar "Security groups" na aba lateral esquerda para ir ao console de "Grupos de segurança" e, então, executar o comando "Criar grupo de segurança".

Após o comando ser dado, deve-se selecionar a VPC onde o grupo de segurança será criado, dar nome e descrição para ele e finalizar com o comando "Criar grupo de segurança".

6.2.2. Edição de grupo de segurança

Para editar um grupo de segurança, deve-se ir ao console de "grupo de segurança", selecionar o grupo a ser editado, selecionar a aba "Regras de entrada" (ou "Regras de saída" caso a regra a editar seja de saída) e dar o comando "Editar regras de entrada" (ou "Editar regras de saída").

Com isso, pode-se acrescentar novas regras, modificá-las ou removê-las. A edição é finalizada com o comando "Salvar regras".

6.2.3. Associação de grupo de segurança

Após um grupo de segurança ser criado, uma instância pode aplicar este grupo. A partir da tela inicial do console da AWS, deve-se procurar pelo console do EC2. De lá deve-se selecionar a instância que aplicará o grupo de segurança.

Selecionada a instância, deve-se executar o comando "Ações", selecionar a opção "Segurança" e, depois, a opção "Alterar grupo de segurança". Lá, deve-se selecionar o grupo de segurança desejado para a instância e pressionar "Salvar".

6.3. Access Control List

A AWS permite a criação de listas de controle de acesso associadas a sub-redes. Uma lista de acesso controla o tipo de tráfego que pode entrar e sair da rede.

Este serviço não examina o tráfego que não atravessa a fronteira da rede (como o tráfego entre instâncias dentro da mesma sub-rede - para controle de tráfego interno, deve-se usar grupos de segurança).

Do mesmo modo que os grupos de segurança, as listas de acesso podem ser aplicadas a diversas sub-redes.

6.3.1. Criação de lista de acesso

Para criar uma lista de acesso, a partir da tela inicial do console da AWS, deve-se procurar pelo console do VCP. De lá deve-se selecionar "Network ACL" para ir ao console de "Network ACLs". Neste momento, deve-se dar o comando "Criar Network ACL".

Após o comando ser dado, deve-se especificar a VPC onde a lista será criada, dar um nome para a lista de acesso e executar o comando "Criar Network ACL".

6.3.2. Editar listas de acesso

Para editar uma lista de acesso, deve-se ir ao console de "Network ACLs", selecionar a lista a ser editada, selecionar a aba "Regras de entrada" (ou "Regras de saída" caso a regra a editar seja de saída) e dar o comando "Editar regras de entrada" (ou "Editar regras de saída").

Com isso, pode-se acrescentar novas regras, modificá-las ou removê-las. A edição é finalizada com o comando "Salvar regras".

6.3.3. Aplicar listas de acesso

Após uma lista de acesso ser criada, uma sub-rede pode aplicá-la. A partir da tela inicial do console da AWS, deve-se procurar pelo console do VCP. De lá deve-se selecionar "Sub-redes" para ir ao console de "Sub-redes". Neste momento, deve-se selecionar a Sub-rede onde a lista de acesso deverá ser aplicada.

Uma vez selecionada a Sub-rede, deve-se ir para a aba Network ACL. Lá, deve-se dar o comando Editar Associação de Network ACL e selecionar o ID da Network ACL que se deseja aplicar na Sub-rede e pressionar "Salvar" para fazer a alteração.

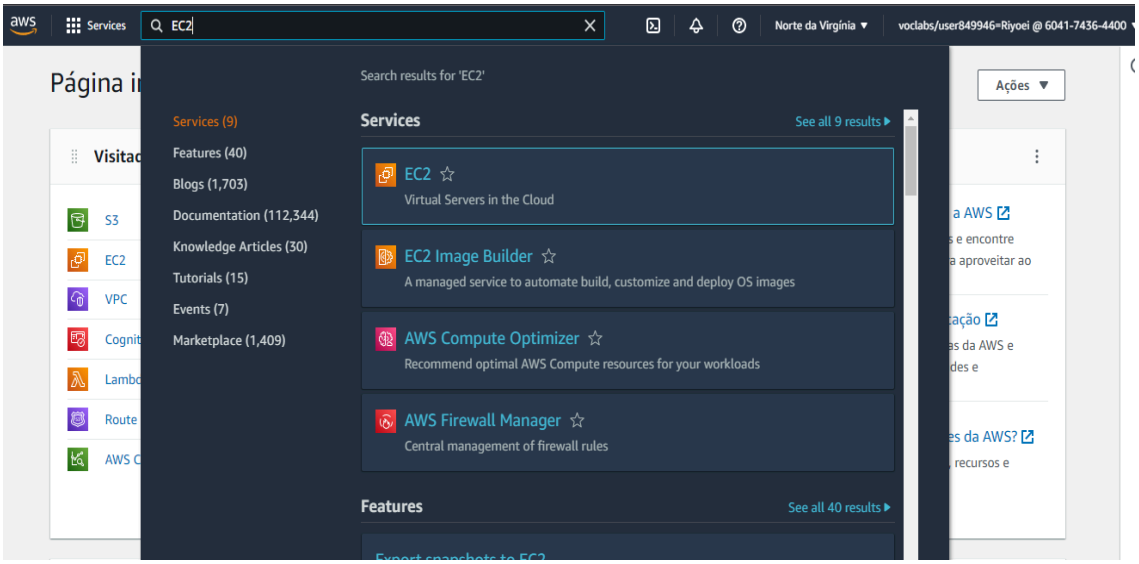
6.4. Demonstração: Servidor Web na Nuvem AWS

Vamos demonstrar como uma instância de máquina virtual pode ser configurada como um servidor web e como a configuração de segurança deste servidor deve ser feita na nuvem da AWS.

6.4.1. Criação de uma instância

A primeira coisa a fazer é ir ao console do EC2 (a partir da tela inicial pode usar o diálogo de busca e procurar por EC2 ou entrar pelo menu de serviços de computação) – veja a Figura 1.

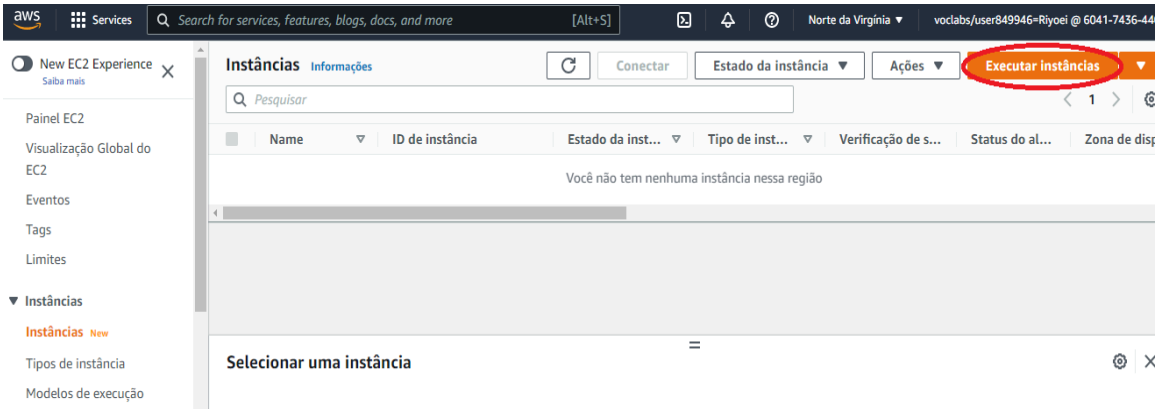
Figura 1. Tela Inicial do Console da AWS



Fonte: https://console.aws.amazon.com/console/home?region=us-east-1#

No console do EC2, deve executar a ação de "Executar Instâncias" – veja a Figura 2.

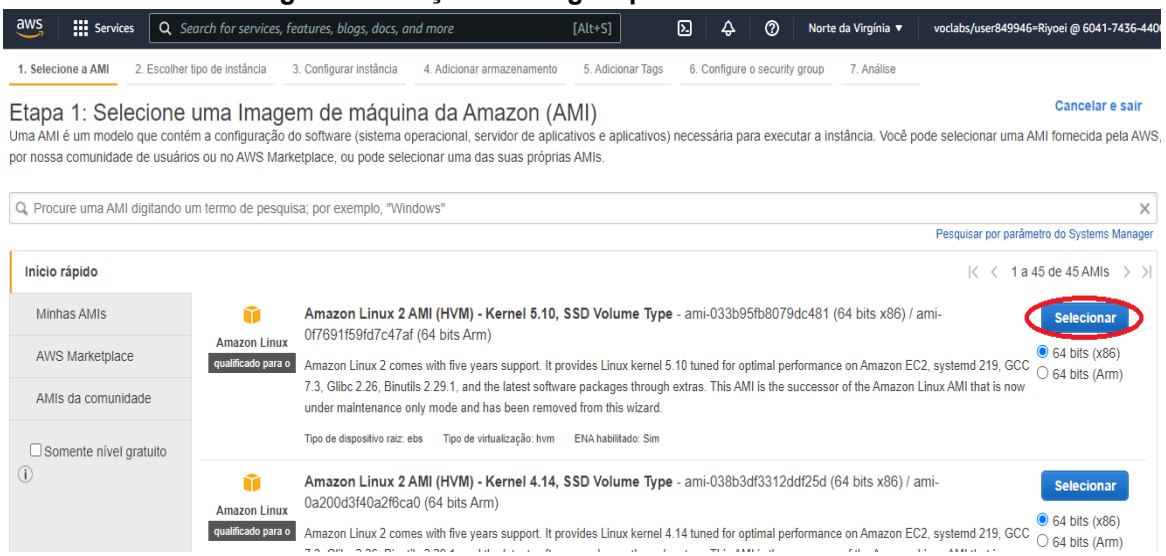
Figura 2. Console do serviço EC2



Fonte: https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:v=3

Na Etapa 1, “Selecione a AMI”, encontre Amazon Linux 2 AMI e pressione “Selecionar” – veja a Figura 3.

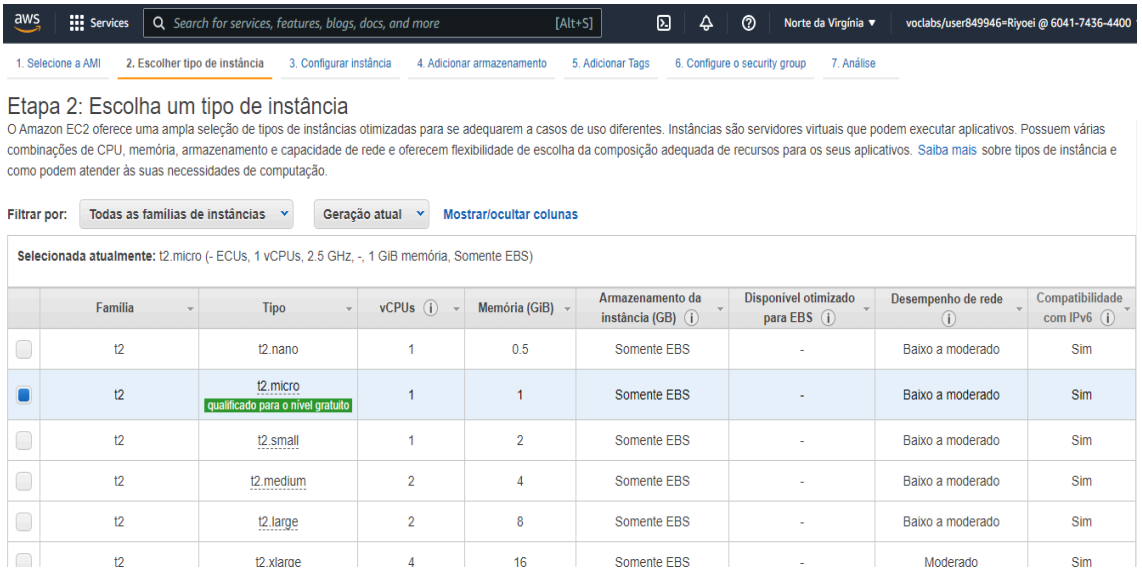
Figura 3. Seleção de Imagem para nova instância



Fonte: https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

Na Etapa 2, “Escolher tipo de instância”, selecione t2.micro (seleção default) e pressione “Próximo: Configure os detalhes da instância” – veja na Figura 4.

Figura 4. Seleção de tipo de instância



Fonte: https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

Mantenha os defaults para a Etapa 3 e pressione "Adicionar armazenamento".

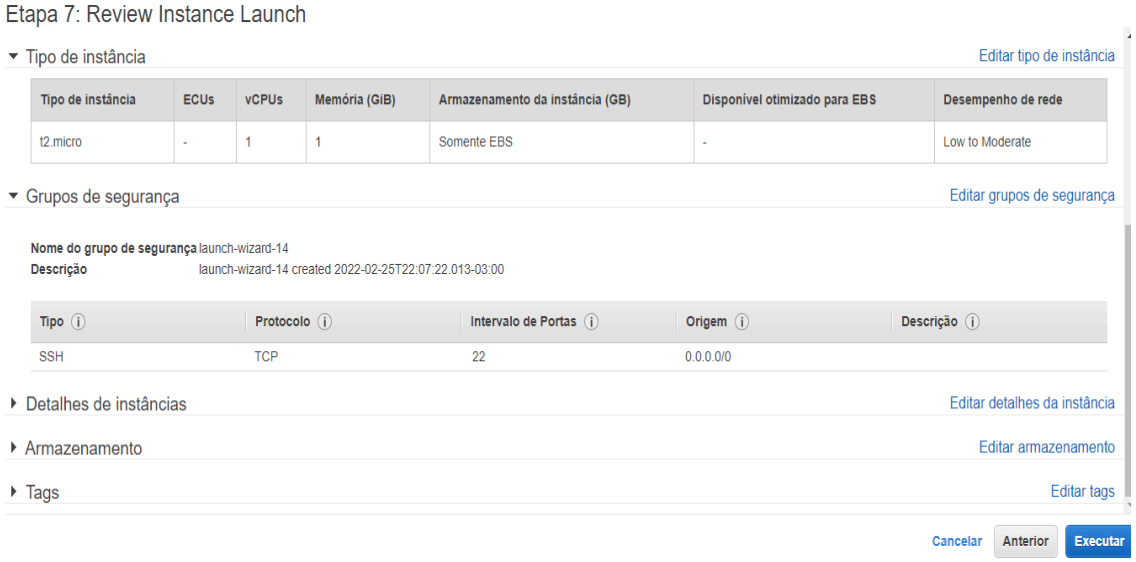
Mantenha os defaults para a Etapa 4 e pressione "Próximo: Adicionar Tags".

Na Etapa 5, adicione a chave "Name" com valor "MeuServidorWEB" e pressione "Próximo: Configure o security group".

Na Etapa 6, mude o nome do grupo de segurança para "SegurancaParaWEB" e pressione "Verificar e ativar".

Na Etapa 7, "Análise", pressione "Executar". Marque o diálogo "Confirmo que tenho acesso ao arquivo de chave privada correspondente e que, sem esse arquivo, não poderei fazer login na minha instância." e pressione "Executar instâncias" – veja na Figura 5.

Figura 5. Análise e ativação da instância

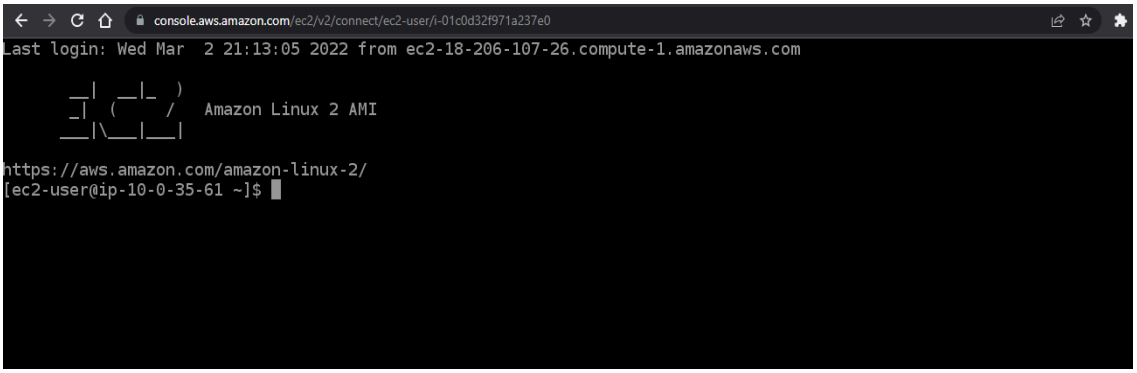


Fonte: do autor, 2022.

Se nada deu errado, a mensagem "Sua instância está sendo iniciada" será exibida. Volte ao console do EC2 que agora mostrará o status da nova instância, com o nome "MeuServidorWEB", em execução.

Para entrar no console da instância, selecione a instância e pressione "Conectar", selecione "Conexão da instância do EC2" e pressione "Conectar". Se funcionou corretamente, uma nova aba do browser será aberta e a tela do console da instância aparecerá. – veja na Figura 6.

Figura 6. Console da instância Linux



Fonte: https://console.aws.amazon.com/ec2/v2/connect/ec2-user/i-01c0d32f971a237e0

6.4.2. Instalação de um servidor WEB na instância

Para instalar um servidor WEB, bastam executar os cinco comandos listados abaixo:
sudo yum update -y
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
cat /etc/system-release
sudo yum install -y httpd
sudo systemctl start httpd

6.4.3. Configuração de grupo de segurança

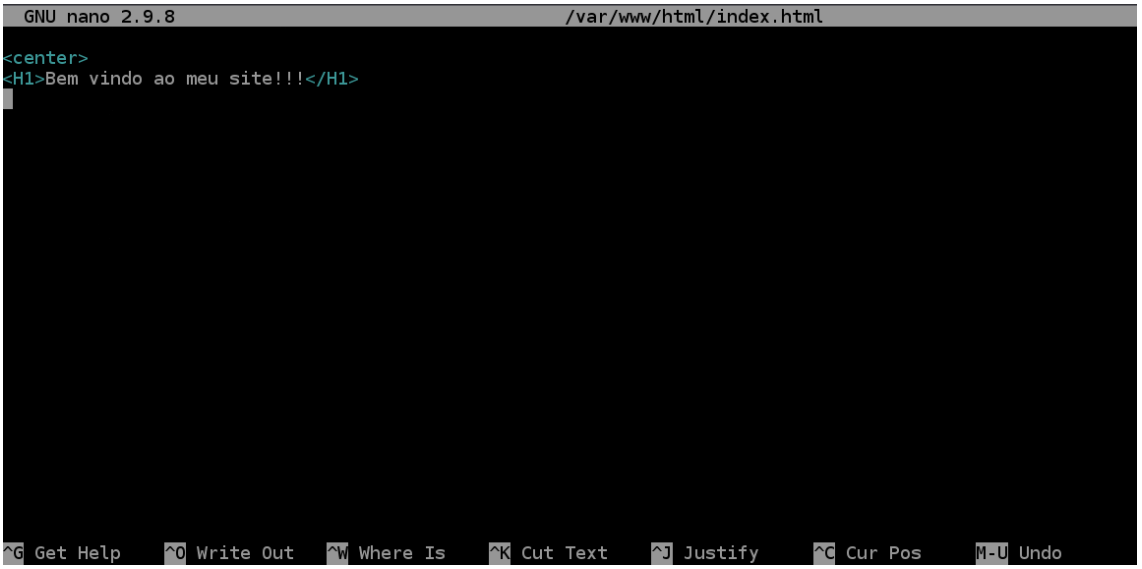
Para que o servidor WEB possa ser acessado, é preciso alterar o grupo de segurança para permitir tráfego HTTP. Para isso, deve-se ir ao console de "Network ACLs", selecionar a lista "SegurancaParaWEB", selecionar a aba "Regras de entrada" e dar o comando "Editar regras de entrada" e "Adicionar Regra".

Ajusta-se a regra para tipo: "HTTP" e origem: "Qualquer local-IPv4" e finaliza com o comando "Salvar regras".

6.4.4. Criação de um site

Para editar a página do site, deve-se dar o comando abaixo:
sudo nano /var/www/html/index.html
editar o conteúdo como desejado, salvar com o comando Ctrl-O e sair com o comando Ctrl-X. Veja a Figura 7.

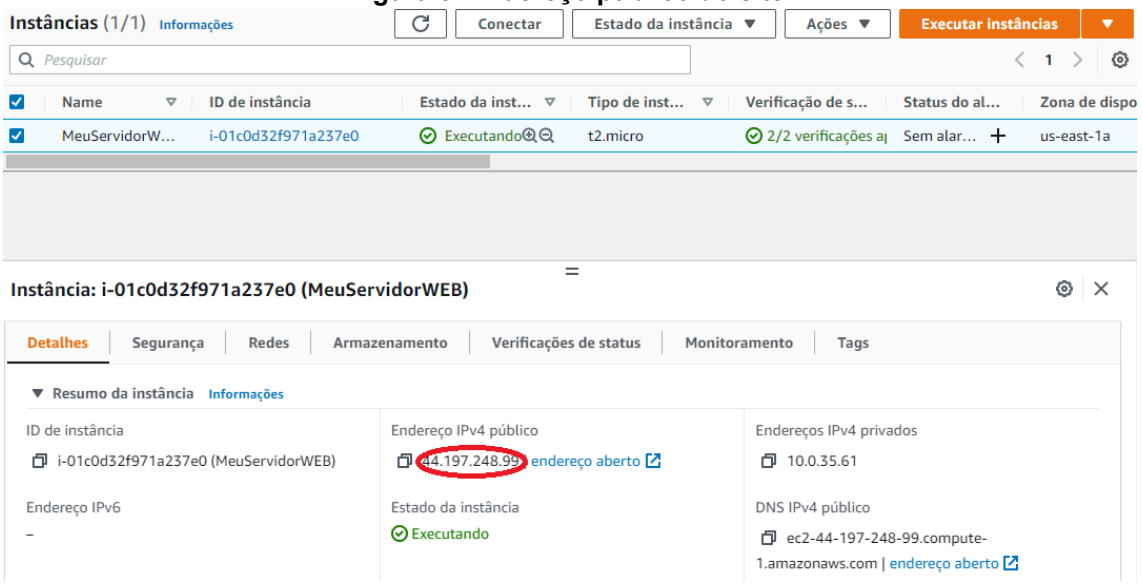
Figura 7. Console da instância Linux



Fonte: https://console.aws.amazon.com/ec2/v2/connect/ec2-user/i-01c0d32f971a237e0

Uma vez criada a página, o endereço IP dela pode ser obtido nos detalhes da instância – veja a Figura 8 com o qual o conteúdo pode ser acessado – veja a Figura 9:

Figura 8. Endereço público do site



Fonte: https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:v=3

Figura 9. Exemplo de site

Bem vindo ao meu site!!!

Fonte: http://44.197.248.99/

6.5. Vamos praticar?

6.5.1. Faça o seu servidor Linux de graça por uma ano

Vá para a AWS e veja as condições para o nível gratuito: um conjunto de serviços que você pode usar por um ano para aprender e praticar. Reúna tudo que você aprendeu até agora e coloque uma instância EC2 do tipo t2.micro (do nível gratuito) para funcionar.

https://aws.amazon.com/pt/

6.5.2. Faça o seu site na AWS

Coloque um servidor Apache na instância EC2 criada e faça nele o seu site na Internet. Veja mais detalhes no link:

https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/install-LAMP.html

Quer fazer um site sofisticado, com página com CSS, JavaScript e Banco de Dados? Veja mais detalhes no link:

https://www.w3schools.com/

https://www.w3schools.com/html/default.asp

https://www.w3schools.com/css/default.asp

https://www.w3schools.com/js/default.asp

https://www.w3schools.com/sql/default.asp

6.6. Você quer ler?

6.6.1. Quer saber mais sobre segurança na nuvem?

Segurança na nuvem é muito importante. Quer saber mais sobre segurança na AWS? Veja mais detalhes no link:

https://aws.amazon.com/pt/security/

6.6.2. Quer treinamento em segurança de nuvem?

Segurança é uma das áreas mais importantes para a Tecnologia da Informação. Imagine a segurança na nuvem? Quer obter uma certificação? Veja mais detalhes nos links:

https://cloud.google.com/certification/guides/cloud-security-engineer?hl=pt

https://www.isc2.org/Certifications/CCSP

Referências

TAURION, Cezar. **Cloud Computing:** computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

VELTE, Anthony T.; VELTE, Toby J.; ELSENPRETER, Robert. **Cloud Computing:** a practical approach. EUA:McGraw-Hill, 2010.

MARSHALL, Nick; BROWN, Mike; BLAIR FRITZ, G.; JOHNSON, Ryan. **Mastering VMware vSphere 6.7.** New Jersey: Sybex, 2019. 848p.

SANTOS, Tiago. **Fundamentos da computação em nuvem** (Série Universitária). São Paulo: Editora Senac, 2018. 211p.

ANDREWS, Joshua; HALL, Jon. VMware **Certified Professional Data Center Virtualization on vSphere 6.7 Study Guide:** Exam 2V0-21.19. New Jersey: Sybex, 2020. 640p.

Official Amazon Web Services (AWS) Documentation. **Amazon Elastic Compute Cloud:** User Guide for Linux Instances. Amazon. 2.105p. Disponível em: <https://aws.amazon.com/documentation/ec2/>. Acesso em: 14 jan. 2022.

Official Amazon Web Services (AWS) Documentation. **Amazon Virtual Private Cloud User Guide.** Amazon. 374p. Disponível em: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ug.pdf>. Acesso em: 20 fev. 2022.