

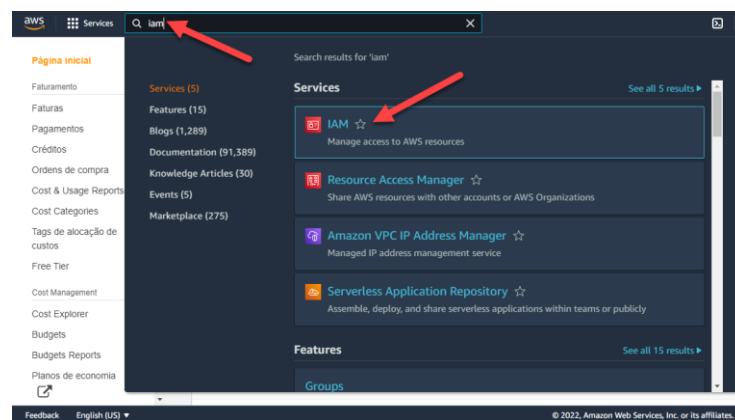
Implantação em Amazon Web Services (AWS) utilizando recurso EC2 de planta virtual utilizando node-red e supervisorio utilizando Scada-LTS.

1. Pré-requisitos
 - 1.1. Ter conta no Amazon Web Services (AWS): <https://aws.amazon.com>
 - 1.2. Conhecimento básico em informática.
2. Fazer download do arquivo do arquivo e descompactar. Vai ser criada a pasta virtualab com dois arquivos, todos os arquivos devem ser salvos e executados dentro dessa pasta. Abaixo segue o link de download.

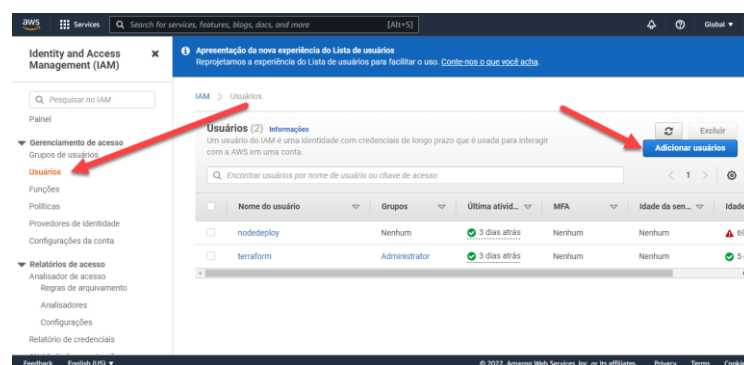
<https://tinyurl.com/virtualabdeploy>

Nome	Data de modificação	Tipo	Tamanho
aws_credentials.txt	24/03/2022 18:54	Documento de Te...	1 KB
virtualab.ps1	24/03/2022 18:54	Script do Window...	1 KB

3. Criar conta de acesso que será utilizado pelo terraform no AWS para criação da infraestrutura.
 - 3.1. Acesse o console da AWS e faça o login com sua conta e pesquise pelo produto IAM (Identity and Access Management).



- 3.2. Iremos criar um usuário para que o terraform possa interagir com a AWS, clique em USERS e em seguida em ADD USER.



- 3.3. Definir detalhes do usuário.

Definir detalhes do usuário

Você pode adicionar vários usuários de uma só vez com o mesmo tipo de acesso e permissões. [Saiba mais](#)

Nome de usuário*

terraform

[+ Adicionar outro usuário](#)

Selecione o tipo de acesso à AWS

Selecione a principal forma de acesso desses usuários à AWS. Se optar somente pelo acesso programático, isso NÃO impedirá que os usuários usem o console com uma função assumida. As chaves de acesso e as senhas geradas automaticamente são fornecidas na última etapa. [Saiba mais](#)

Selecionar tipo de credencial da

AWS*

☒ **Chave de acesso: acesso programático**

Habilita uma **ID da chave de acesso** e **chave de acesso secreta** para a API da AWS, CLI, SDK, e outras ferramentas de desenvolvimento.

☐ **Senha: acesso ao Console de Gerenciamento da AWS**

Habilita uma **senha** que permite que os usuários façam login no Console de Gerenciamento da AWS.

* Obrigatório

[Cancelar](#)

[Próximo: Permissões](#)

3.4. Adicione a política AmazonEC2FullAccess ao usuário, o que dará permissão total ao usuário apenas a recursos da EC2, e clique em Next.

Definir permissões



Adicionar usuário ao grupo



Copiar as permissões de um usuário existente



Anexar políticas existentes de forma direta

[Criar política](#)



Filtrar políticas

ec2full

Exibindo 1 resultado

	Nome da política	Digite	Usado como
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	Gerenciado pela AWS	Nenhum

Definir limite de permissões

[Cancelar](#)

[Anterior](#)

[Próximo: Tags](#)

3.5. Tags são utilizadas para adicionar informações relevantes ao usuário, clique em Next.

Adicionar tags (opcional)

As tags do IAM são pares de chaves/valores que você pode adicionar ao usuário. As tags podem incluir as informações do usuário, como um endereço e-mail, ou podem ser descritivas, como um cargo. Você pode usar as tags para organizar, rastrear ou controlar o acesso para esse usuário. [Saiba mais](#)

Chave	Valor (opcional)	Remover
<input type="text" value="Adicionar nova chave"/>	<input type="text"/>	<input type="button" value="X"/>

Você pode adicionar mais 50 tags.

[Cancelar](#)

[Anterior](#)

[Próximo: Revisar](#)

3.6. Verifique os dados e clique em Create user.

Revisar

Revise suas escolhas. Depois de criar o usuário, você pode visualizar e fazer download da senha e da chave de acesso geradas automaticamente.

Detalhes do usuário

Nome de usuário

terraform

Tipo de acesso AWS

Acesso programático: com uma chave de acesso

Limite de permissões

Limite de permissões não definido

Resumo de permissões

As políticas a seguir serão anexadas ao usuário mostrado acima.

Digite	Nome
Política gerenciada	AmazonEC2FullAccess

Tags

Nenhuma tag foi adicionada.

[Cancelar](#)

[Anterior](#)

[Criar usuário](#)

3.7.Clique em show e copie o Access key ID e Secret access key

Adicionar usuário

1 2 3 4 5

✓ **Êxito**

Você criou com êxito os usuários mostrados abaixo. Você pode visualizar e fazer download das credenciais de segurança do usuário. Você também pode enviar um e-mail aos usuários com as instruções para fazer login no Console de Gerenciamento da AWS. Esta é a última vez que essas credenciais estarão disponíveis para download. No entanto, você pode criar novas credenciais a qualquer momento.

Os usuários com acesso ao Console de Gerenciamento da AWS podem fazer login em:
<https://007556476771.signin.aws.amazon.com/console>

Fazer download .csv

	Usuário	ID da chave de acesso	Chave de acesso secreta
▶	✓ terraform	AKIAQDQTGV5RX4KX2OP2	6eI0p/X8xmEiCuC4wxr83RB4KVPIc4ID+x1o00L+ Ocultar

Fechar

3.8.O usuário criado e chave de acesso não devem ser compartilhados, uma vez que quem tiver acesso a estes dados terá controle sobre os recursos adicionados como política, por questões de segurança este usuário não existe mais em minha conta.

4. Editar arquivo **aws_credentials.txt** e adicionar a chave de acesso e a chave secreta substituindo os valores <access_key> e <secret_access_key>.

```
aws_credentials.txt - Bloco de Notas
Arquivo  Editar  Formatar  Exibir  Ajuda
[default]
aws_access_key_id = <access_key>
aws_secret_access_key = <secret_access_key>
```

5. Acessar o site e gerar par de chaves rsa que será utilizado para conexão ssh.

5.1.Acesso o website <https://www.wpoven.com/tools/create-ssh-key#>

5.2.Configure o type como rsa, length 2048, password deixe em branco e clique em create key.

Generate SSH Key Pair Online

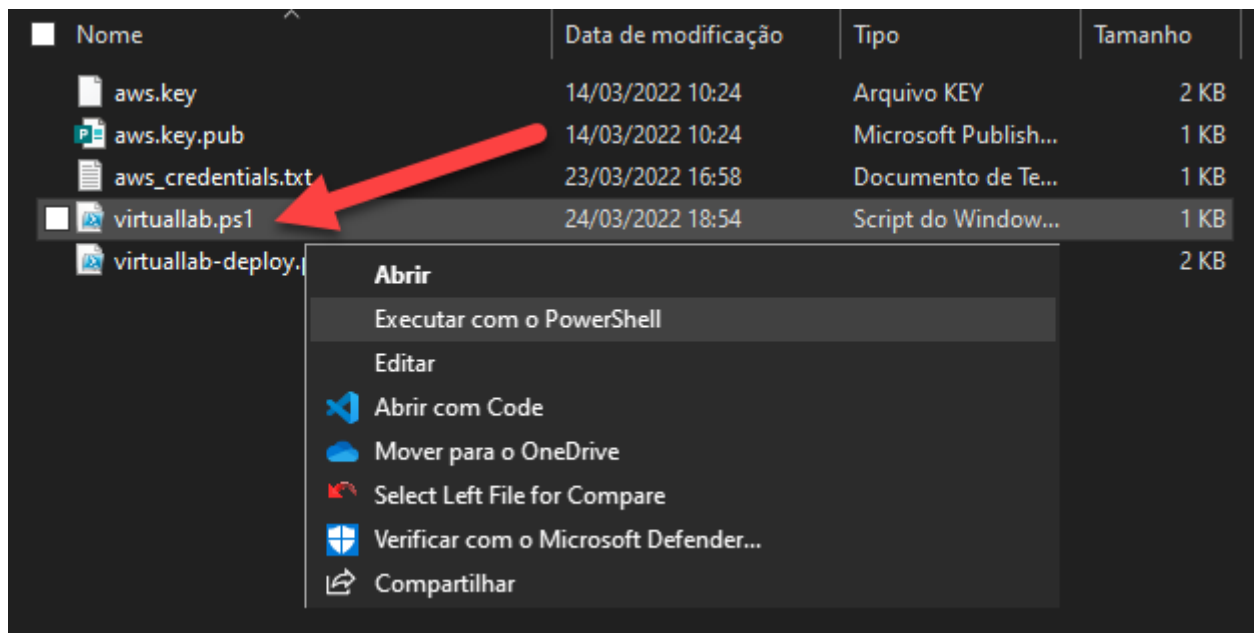
Password Type Length

If password is needed

5.3.Fazer download do **Private Key** e salvar arquivo com nome **aws.key**.

5.4.Fazer download do **Public Key** e salvar arquivo com nome **aws.pub.key**.

6. Clicar com botão direito do mouse do arquivo `virtuallab.ps1` e “Executar com o PowerShell”



7. Vai ser exibido um menu com 3 opções:

7.1.**Opção 1:** Vai subir a infraestrutura do `virtuallab` no `aws`, o processo leva de 7 a 10 minutos para ser implementado e ao final será exibido os endpoints para acesso ao supervisor, `node-red` e caso necessário o comando para acesso via `ssh`. Veja na imagem abaixo um exemplo dos endereços de acesso.

7.2.**Opção 2:** Vai desalocar todos os recursos que foram criados. É muito importante desalocar os recursos após finalizar sua utilização para não ter custos extras.

7.3.**Opção 3:** Sai do menu

```
aws_instance.server: Still creating... [5m0s elapsed]
aws_instance.server: Still creating... [5m10s elapsed]
aws_instance.server (remote-exec): + sudo mv all-databases.sql ./scadalts-data
aws_instance.server: Still creating... [5m20s elapsed]
aws_instance.server (remote-exec): + docker exec -i mysql sh -c 'exec mysql -uroot -proot -f < /var/lib/mysql/all-databa
ses.sql'
aws_instance.server (remote-exec): mysql: [Warning] Using a password on the command line interface can be insecure.
aws_instance.server: Still creating... [5m30s elapsed]
aws_instance.server (remote-exec): ERROR 1146 (42502) at line 2542: Table 'scadalts.plcalarms' doesn't exist
aws_instance.server (remote-exec): ERROR 1146 (42502) at line 2560: Table 'scadalts.plcalarms' doesn't exist
aws_instance.server (remote-exec): + docker stop scadalts
aws_instance.server: Still creating... [5m40s elapsed]
aws_instance.server (remote-exec): scadalts
aws_instance.server: Still creating... [5m50s elapsed]
aws_instance.server (remote-exec): + docker start scadalts
aws_instance.server (remote-exec): scadalts
aws_instance.server (remote-exec): + docker cp ./uploads/5.png scadalts:/usr/local/tomcat/webapps/Scada-LTS/uploads/5.pn
g
aws_instance.server: Creation complete after 5m53s [id=i-09ff591aaa4536904]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Outputs:
nodered = "ec2-34-238-126-127.compute-1.amazonaws.com:1880"
public_dns = "ec2-34-238-126-127.compute-1.amazonaws.com"
public_ip = "34.238.126.127"
scada-lts = "ec2-34-238-126-127.compute-1.amazonaws.com:8080/Scada-LTS"
ssh_connection = "ssh -i aws_key ec2-user@ec2-34-238-126-127.compute-1.amazonaws.com"
PS C:\temp\virtual-lab-deploy\aws>
```