AUTOR:	Josely Castro
DATA CRIAÇÃO:	17/01/2025
ÚLTIMA REVISÃO:	17/01/2025
REVISADO POR:	Hitalo Aquino
STATUS:	Ativo
TÍTULO:	Laboratório 7. Monitoramento e Auditoria com CloudWatch e CloudTrail

Objetivos:

Este laboratório ensina como configurar:

- **Alarme CloudWatch:** Monitorar a CPU de uma instância EC2 e enviar notificações por e-mail (SNS) quando um limite for atingido.
- **CloudTrail:** Habilitar a auditoria (rastreamento de eventos) na sua conta AWS e armazenar os logs em um bucket S3.
- **Visualização de Logs:** Acessar os logs do CloudTrail.

Cenário:

Você precisa monitorar o desempenho de uma instância EC2 e ser alertado sobre alta utilização de CPU. Também precisa manter um registro de auditoria de todas as atividades na sua conta AWS para segurança e conformidade.

Pré-requisitos:

- **Conta AWS:** Conta ativa com permissões para EC2, CloudWatch, CloudTrail, SNS e S3.
- Permissões IAM: CloudWatchFullAccess, AWSCloudTrail_FullAccess, AmazonSNSFullAccess, AmazonS3FullAccess, AmazonEC2FullAccess.
- Navegador Web.

Tarefas

Passo 1:

- **Console EC2:** Acesse o console do EC2.
- **Launch Instance:**
  - **Name:** Instancia-Teste-CloudWatch
  - **AMI: Amazon Linux 2 AMI (HVM)** - x86_64.
  - **Instance type:** t2.micro
  - **Key pair:** Selecione/crie. **(Você vai precisar acessar a instância, então saiba onde está salva o seu par de chaves).**

    - **Network settings:**
        - **VPC:** Sua *VPC padrão*.
        - **Subnet:** Qualquer sub-rede *pública*.
        - **Auto-assign public IP:** Enable.
        - **Firewall:**
            - **Create security group:**
            - **Name:** SG-Teste-CloudWatch-SeuNome
            - **Inbound:** SSH, Source: My IP
    - **Configure storage:** Padrão.
    - **Advanced details:** Nada.
- **Launch Instance.**
- **Anote o Instance ID.**

Passo 2:

- **Console CloudWatch:** Acesse o console do CloudWatch.
- **Criar Alarme:**
    - **Alarms -> Create alarm.**
    - **Select metric:**
        - **All metrics -> EC2 -> Per-Instance Metrics**.
        - *Cole o ID da instância (anotada do passo anterior)* na caixa de pesquisa.
        - Marque CPUUtilization *da sua instância*.
        - Aba **Graphed metrics (1)**: Verifique.
        - **Select metric.**
    - **Specify metric and conditions:**
        - **Statistic:** Average.
        - **Period:** 5 minutes.
        - **Conditions:**
            - **Threshold type:** Static.
            - **Whenever CPUUtilization is...:** Greater.
            - **than...:** 70.
        - **Additional configuration:**
            - **Datapoints to alarm:** 1 out of 1.
            - **Missing data treatment:** Treat missing data as good (not breaching threshold).
        - **Next.**
    - **Configure actions:**
        - **Alarm state trigger:** In alarm.
        - **Select an SNS topic:** Crie um tópico SNS (*confirme a assinatura*).
        - **Next.**
    - **Add a name and description:**
        - **Alarm name:** AlarmeCPU-Instancia-SeuNome
        - **Next.**
    - **Preview and create:** Revise e **Create alarm.**

Passo 3:

- **Console CloudTrail:** Acesse o console do CloudTrail.

- **Criar uma Trilha (Trail):**
    - **Trails** -> **Create trail**.
    - **Step 1: Choose trail attributes:**
        - **Trail name:** trilha-auditoria-seunome
        - **Storage location:**
            - **Create a new S3 bucket.**
            - **Trail log bucket and folder:** O CloudTrail *sugerirá* um nome.
            - **Log file SSE-KMS encryption:** *Marque* (**Enabled**).
                - **Customer managed AWS KMS key:** New.
                - **AWS KMS alias:** alias/CloudTrailKey-seunome.
        - **Additional settings:**
            - **Log file validation:** Deixe habilitado.
            - **SNS notification delivery:** Deixe desabilitado.
            - **CloudWatch Logs:** Deixe desabilitado.
        - Clique em **Next.**
    - **Step 2: Choose log events:**
        - **Event type:**
            - **Management events:** *Mantenha marcado*.
                - **API activity:** *Mantenha* **Read** e **Write**.
            - **Data events:** *Desmarque*.
            - **Insights events:** *Desmarque*.
            - **Network activity events:** *Desmarque*.
        - Clique em **Next.**
    - **Step 3: Review and create:** Revise e **Create trail**.

Passo 4:

- **Logs do CloudTrail (no S3 - Padrão):**
    - Acesse o console do S3.
    - Localize o bucket criado pelo CloudTrail.
    - Navegue pela estrutura de pastas para encontrar os logs (arquivos .gz JSON).
- **(Opcional) Enviar Logs do CloudTrail para o CloudWatch Logs:**
  * Console do *CloudTrail* -> **Trails** -> Sua trilha.
  * Seção **CloudWatch Logs** -> **Edit.**
  * **CloudWatch Logs:** *Marque* (**Enabled**).
  * **Log group:** Crie um novo (ex: CloudTrail/Logs-SeuNome).
  * **IAM Role:** Crie um novo: CloudTrailRoleForCloudWatchLogs, clique me Allow.
  * **Save changes.**
- **Logs no CloudWatch Logs (se configurado):**
    - **Console CloudWatch: Logs** -> **Log groups.**
    - **Visualizar Logs:** Clique no grupo de logs.

Passo 5:

- **Conectar-se à Instância (SSH):** Use SSH.
- **Instalar o stress:**

```
sudo yum update -y

sudo amazon-linux-extras install epel -y  # Amazon Linux 2

sudo yum install stress -y
```

- **Executar o stress:**

```
stress --cpu 8 --timeout 600
```

Passo 5:

- **Monitorar:** Veja o CloudWatch e aguarde o e-mail. **(Tire print e anexe na entrega da atividade no classroom)**
- **Parar o stress:** Ctrl+C.

Passo 6:

1. Exclua o Alarme CloudWatch.
2. Exclua a Trilha do CloudTrail.
3. Exclua o Bucket S3 do CloudTrail (se criou um novo - *esvazie antes de excluir*).
4. Exclua o tópico do SNS (se criou).
5. *Pare ou termine* a instância EC2.