

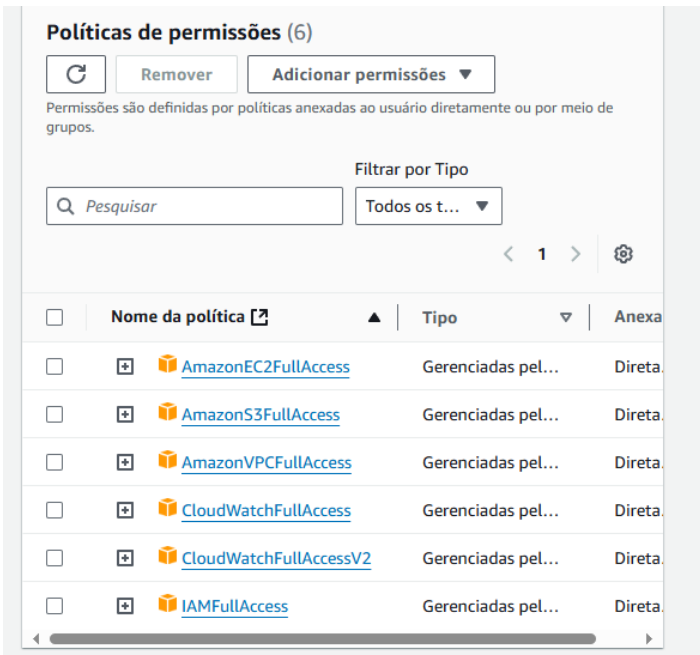
Relatório prova do dia – 08/11/2024

Usuário para correção:

URL de login do console: <https://010526242675.signin.aws.amazon.com/console>

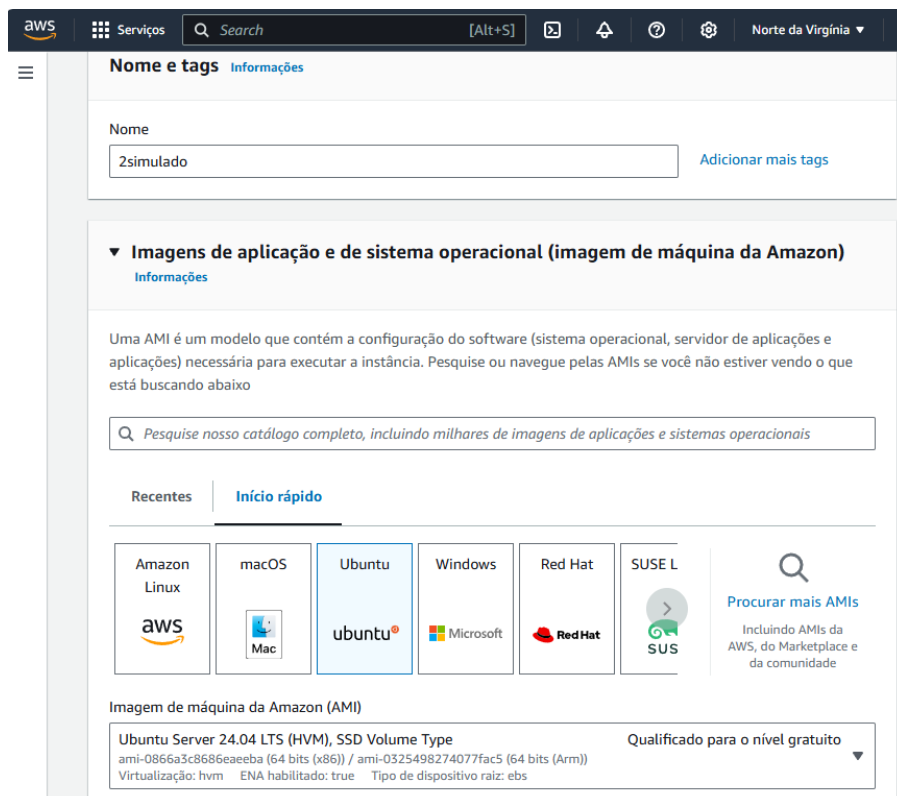
Nome do user: correcaoUser

Senha: correcaoOc#53



1- Criação da Instância EC2

Criação da instância:



▼ Tipo de instância

Informações | Obter conselhos

Tipo de instância

t2.micro

Qualificado para o nível gratuito

Família: t2 1 vCPU 1 GiB Memória Geração atual: true

Sob demanda Windows base definição de preço: 0.0162 USD por hora

Sob demanda Ubuntu Pro base definição de preço: 0.0134 USD por hora

Sob demanda SUSE base definição de preço: 0.0116 USD por hora

Sob demanda RHEL base definição de preço: 0.026 USD por hora

Sob demanda Linux base definição de preço: 0.0116 USD por hora

Todas as gerações

Comparar tipos de instância

Custos adicionais aplicáveis a AMIs com software pré-instalado

Criei um security Group com regras específicas:

▼ Configurações de rede

Informações

Editar

Rede

Informações

vpc-0850d9d811cee3443

Sub-rede

Informações

Sem preferência (sub-rede padrão em qualquer zona de disponibilidade)

Atribuir IP público automaticamente

Informações

Habilitar

Taxas adicionais se aplicam quando fora do limite de nível gratuito

Firewall (grupos de segurança)

Informações

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☐ Criar grupo de segurança

☒ Selecionar grupo de segurança existente

Grupos de segurança comuns

Informações

Selecionar grupos de segurança

securityGroup-2simulado sg-096144632a8397fea X

VPC: vpc-0850d9d811cee3443

Comparar regras do grupo de segurança

Os grupos de segurança que você adicionar ou remover aqui serão adicionados ou removidos em todas as suas interfaces de rede.

Regras atribuídas ao Security Group são mostradas abaixo na etapa 2.

Criação da VPC:

▼ Nuvem privada virtual

Suas VPCs

- Sub-redes
- Tabelas de rotas
- Gateways da Internet
- Gateways da Internet somente de saída
- Gateways da operadora
- Conjuntos de opções de DHCP
- IPs elásticos
- Listas de prefixos gerenciados
- Endpoints
- Serviços de endpoint
- Gateways NAT
- Conexões de emparelhamento

▼ Segurança

- ACLs da rede
- Grupos de segurança

▼ Firewall de DNS

- Grupos de regras
- Listas de domínios

▼ Network Firewall

- Firewalls

VPC-2simulado [vpc-0ffd909b7b6a0d508](#) Available 10.0.0.0/24

vpc-0ffd909b7b6a0d508 / VPC-2simulado

Detalhes | Mapa de recursos | CIDRs | Logs de fluxos | Tags | Integrações

Detalhes			
ID da VPC vpc-0ffd909b7b6a0d508	Estado Available	Nomes de host DNS Desabilitado	Resolução de DNS Habilitado
Localização Default	Conjunto de opções de DHCP dopt-09f710085a3c99548	Tabela de rota principal -	Network ACL principal -
VPC padrão Não	CIDR IPv4 10.0.0.0/24	Grupo IPv6 -	CIDR IPv6 (Grupo de borda de rede) -
Métricas de uso do		ID do proprietário	

Subnet:

public subnet - 2simulado [subnet-0237c4734bb10fc4b](#) Available 10.0.0.0/24

subnet-0237c4734bb10fc4b / public subnet - 2simulado

Detalhes | Logs de fluxos | Tabela de rotas | Network ACL | Reservas CIDR

Detalhes			
ID da sub-rede subnet-0237c4734bb10fc4b	ARN da sub-rede arn:aws:ec2:us-east-1:010526242675:subnet/subnet-0237c4734bb10fc4b	Estado Available	CIDR IPv4 10.0.0.0/24
Endereços IPv4 disponíveis 251	CIDR IPv6 -	ID da associação de CIDR IPv6 -	Zona de disponibilidade us-east-1a
ID de zona de disponibilidade use1-az2	Grupo de borda de rede	VPC vpc-0ffd909b7b6a0d508 VPC-2simulado	Tabela de rotas -
Network ACL		Atribuir endereço IPv6 automaticamente	

ID da instância: [i-02119ed2945c6f89d](#)

Endereço de IP atribuído: 44.201.87.149

2- Configuração de Segurança

Regra de saída 1

Excluir

ID da regra do grupo de segurança
sgr-0aa9c24f750ab39c9

Tipo [Informações](#)
HTTPS

Protocolo [Informações](#)
TCP

Intervalo de portas [Informações](#)
443

Tipo de destino [Informações](#)
Qualquer local-IPv4

Destino [Informações](#)
0.0.0.0/0

Descrição - opcional [Informações](#)

Regra de saída 2

Excluir

ID da regra do grupo de segurança
sgr-029da2a4057f126d6

Tipo [Informações](#)
SSH

Protocolo [Informações](#)
TCP

Intervalo de portas [Informações](#)
22

Tipo de destino [Informações](#)
Meu IP

Destino [Informações](#)
187.103.65.130/32

Descrição - opcional [Informações](#)

Regra de saída 3

Excluir

ID da regra do grupo de segurança
sgr-018e8923025aebec4

Tipo [Informações](#)
HTTP

Protocolo [Informações](#)
TCP

Intervalo de portas [Informações](#)
80

Tipo de destino [Informações](#)
Qualquer local-IPv4

Destino [Informações](#)
0.0.0.0/0

Descrição - opcional [Informações](#)

Resposta da pergunta: Elas deixam a instância mais segura, permitindo o acesso apenas aos IPs estabelecidos pelo arquiteto.

3- Configuração de ACL de Rede

ACL-2simulado

acl-0434d6e347c9508c8

acl-0434d6e347c9508c8 / ACL-2simulado

Detalhes

Regras de entrada

Regras de saída

Associações de sub-rede

Tags

Detalhes

ID da Network ACL

acl-0434d6e347c9508c8

Proprietário

010526242675

Associado a

-

Padrão

Não

ID da VPC

[vpc-0ff909b7b6a0d508](#) / [VPC-2simulado](#)

Tráfegos de ENTRADA *PERMITIDOS*

VPC

Network ACLs

acl-0434d6e347c9508c8 / ACL-2simulado

Editar regras de entrada

Editar regras de entrada

Informações

Regras de entrada controlam o tráfego de entrada que tem permissão para acessar a VPC.

Regra de entrada 1

Número da regra

Informações

1

Tipo

Informações

SSH (22)

Protocolo

Informações

TCP (6)

Intervalo de portas

Informações

22

Origem

Informações

0.0.0.0/0

Permitir/negar

Informações

Permitir

Remover

Regra de entrada 2

Número da regra

Informações

2

Tipo

Informações

HTTP (80)

Protocolo

Informações

TCP (6)

Intervalo de portas

Informações

80

Origem

Informações

0.0.0.0/0

Permitir/negar

Informações

Permitir

Remover

Regra de entrada 3

Número da regra

Informações

3

Tipo

Informações

HTTPS (443)

Protocolo

Informações

TCP (6)

Intervalo de portas

Informações

443

Origem

Informações

0.0.0.0/0

Permitir/negar

Informações

Permitir

Remover

Tráfegos de ENTRADA *NEGADOS*

Regra de entrada 4

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

4

Todos os TCP

TCP (6)

Intervalo de portas [Informações](#)

Origem [Informações](#)

Permitir/negar [Informações](#)

Tudo

0.0.0.0/0

Negar

Remover

Regra de entrada 5

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

5

Todos os ICMPs - IPv6

IPv6-ICMP (58)

Intervalo de portas [Informações](#)

Origem [Informações](#)

Permitir/negar [Informações](#)

Tudo

0.0.0.0/0

Negar

Remover

Regra de entrada 6

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

*

Todo o tráfego

Tudo

Intervalo de portas [Informações](#)

Origem [Informações](#)

Permitir/negar [Informações](#)

Tudo

0.0.0.0/0

Negar

Adicionar nova regra

Classificar por número de regra

Tráfegos de SAÍDA *PERMITIDOS*

VPC > [Network ACLs](#) > [acl-0434d6e347c9508c8](#) / [ACL-2simulado](#) > Editar regras de saída

Editar regras de saída [Informações](#)

Regras de saída controlam o tráfego de saída que tem permissão para sair da VPC.

Regra de saída 1

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

1

SSH (22)

TCP (6)

Intervalo de portas [Informações](#)

Destino [Informações](#)

Permitir/negar [Informações](#)

22

0.0.0.0/0

Permitir

Remover

Regra de saída 2

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

2

HTTP (80)

TCP (6)

Intervalo de portas [Informações](#)

Destino [Informações](#)

Permitir/negar [Informações](#)

80

0.0.0.0/0

Permitir

Remover

Regra de saída 3

Número da regra [Informações](#)

Tipo [Informações](#)

Protocolo [Informações](#)

3

HTTPS (443)

TCP (6)

Intervalo de portas [Informações](#)

Destino [Informações](#)

Permitir/negar [Informações](#)

443

0.0.0.0/0

Permitir

Remover

Tráfegos de SAÍDA *NEGADOS*

Regra de saída 4

Número da regra [Informações](#)
4

Tipo [Informações](#)
Todos os TCP

Protocolo [Informações](#)
TCP (6)

Intervalo de portas [Informações](#)
Tudo

Destino [Informações](#)
0.0.0.0/0

Permitir/negar [Informações](#)
Negar

Remover

Regra de saída 5

Número da regra [Informações](#)
5

Tipo [Informações](#)
Todos os ICMPs - IPv6

Protocolo [Informações](#)
IPv6-ICMP (58)

Intervalo de portas [Informações](#)
Tudo

Destino [Informações](#)
0.0.0.0/0

Permitir/negar [Informações](#)
Negar

Remover

Regra de saída 6

Número da regra [Informações](#)
*

Tipo [Informações](#)
Todo o tráfego

Protocolo [Informações](#)
Tudo

Intervalo de portas [Informações](#)
Tudo

Destino [Informações](#)
0.0.0.0/0

Permitir/negar [Informações](#)
Negar

Você deve instalar ferramentas de monitoramento na instância Ubuntu para acompanhar seu desempenho. – Não conseguiu fazer

Ativar monitoramento detalhado para a instância EC2:

Painel

Visualização Global do EC2

Eventos

▼ Instâncias

Instâncias

Tipos de instância

Modelos de execução

Solicitações spot

Savings Plans

Instâncias reservadas

Hosts dedicados

Reservas de capacidade [Novo](#)

▼ Imagens

AMIs

Catálogo de AMIs

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Rede e segurança

Security groups

IPs elásticos

Placement groups

Pares de chaves

Interfaces de rede

▼ Balanceamento de carga

Load balancers

Grupos de destino

Instâncias (1/1) [Informações](#)

Última atualização less than a minute atrás

Conectar

Estado da instância ▼

Ações ▼

Executar instâncias ▼

Localizar instância por atributo ou tag (case-sensitive)

Todos os estados ▼

< 1 >

⚙

<input checked="" type="checkbox"/>	Name	ID da instância	Estado da inst...	Tipo de inst...	Verif
<input checked="" type="checkbox"/>	2simulado	i-02119ed2945c6f89d	Executando	t2.micro	2

Monitoramento detalhado

Depois de habilitar o monitoramento detalhado para uma instância, os dados de monitoramento ficam disponíveis em períodos de 1 minuto. [Saiba mais](#)

ID da instância

☒ i-02119ed2945c6f89d (2simulado)

Monitoramento detalhado

☒ Habilitar

Após habilitar o monitoramento detalhado, o console do Amazon EC2 exibe gráficos de monitoramento com um período de 1 minuto para a instância. [Cobranças adicionais aplicáveis](#)

Cancelar

Confirmar

Detalhe

Incluir m [Saiba m](#)

Recomendações de alarme

3h 1d 1sem

Fuso horário ... ▼

ne ao pai nel

Utilização ...

Entrada d...

Saída de r...

Entrada

Percent

Bytes

Bytes

Count

8.27

86.1k

6.47k

78.8

4.14

43.0k

3.23k

39.4

0

0

0

0

13:05

14:05

13:05

14:05

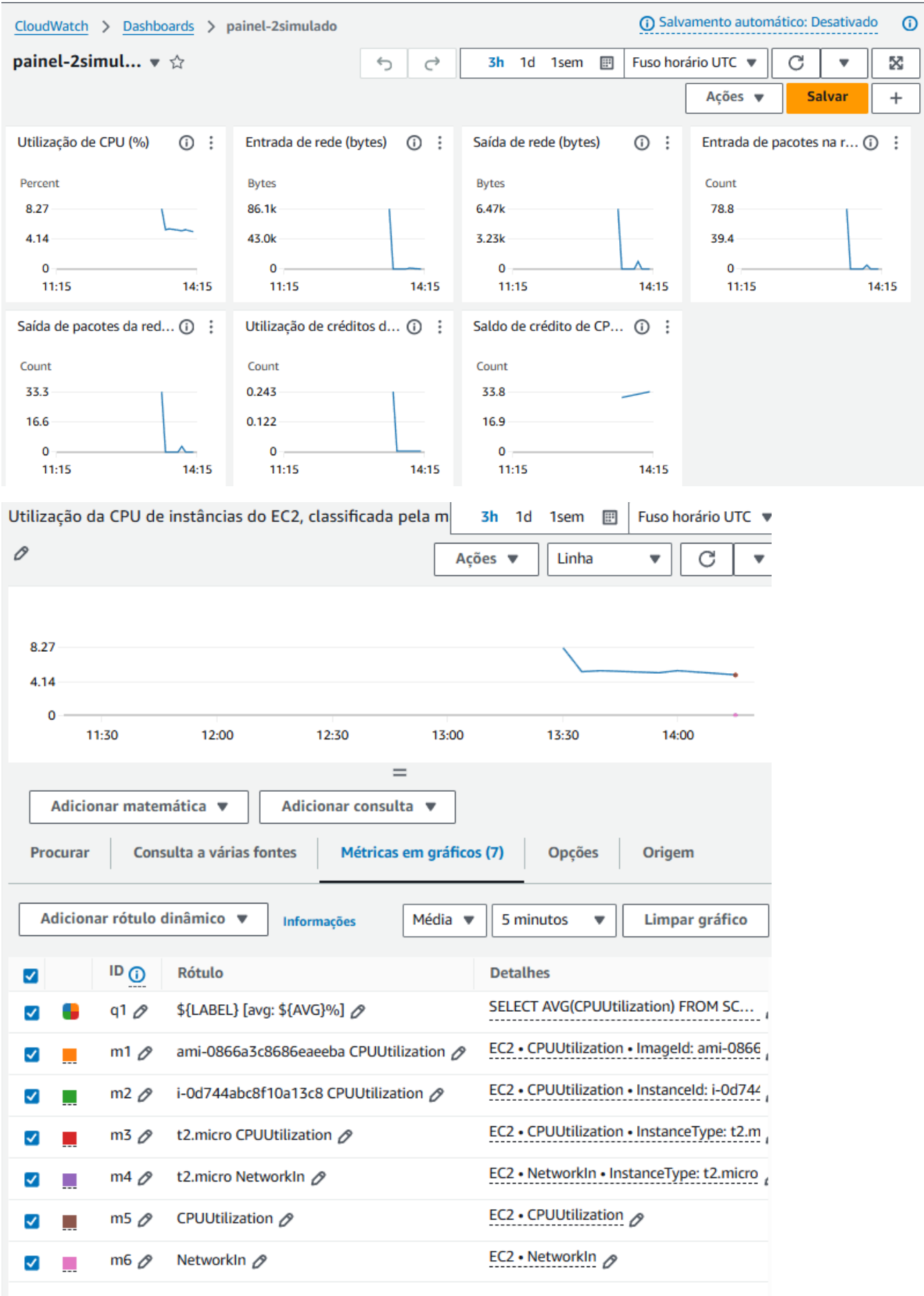
13:05

14:05

13:05

14:05

Painel do monitoramento da instância:



4- Criação de Políticas e IAM

The screenshot shows the 'Create New Policy' wizard in the AWS IAM console. It is at the 'Select a service or use case' step. At the top, there are three radio button options: 'Identidade Web' (selected), 'Federação SAML 2.0', and 'Política de confiança personalizada'. Below these, the 'Caso de uso' (Use case) section is expanded, showing a dropdown menu with 'EC2' selected. Underneath, a list of use cases for EC2 is provided, with 'EC2' selected by default. At the bottom right, there are 'Cancelar' (Cancel) and 'Próximo' (Next) buttons.

☐ Identidade Web
Permite que os usuários federados pelo provedor de identidade da Web externo assumam essa função para executar ações nessa conta.

☐ Federação SAML 2.0
Permitir que os usuários federados com o SAML 2.0 de um diretório corporativo executem ações nessa conta.

☐ Política de confiança personalizada
Crie uma política de confiança personalizada para permitir que outras pessoas executem ações nessa conta.

Caso de uso
Permitir que um serviço da AWS, como o EC2, o Lambda ou outros executem ações nessa conta.

Serviço ou caso de uso
EC2 ▼

Escolha um caso de uso para o serviço especificado.
Caso de uso

- ☒ EC2
Allows EC2 instances to call AWS services on your behalf.
- ☐ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- ☐ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- ☐ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- ☐ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- ☐ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- ☐ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- ☐ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancelar Próximo

Permissões:

The screenshot shows the 'Add Permissions' step (Etapa 2) in the AWS IAM console. It features a table titled 'Resumo da política de permissões' (Summary of the permission policy). The table has three columns: 'Nome da política' (Policy name), 'Tipo' (Type), and 'Anexado como' (Attached as). Two policies are listed: 'AmazonS3ReadOnlyAccess' and 'CloudWatchReadOnlyAccess', both of type 'Gerenciadas pela AWS' (Managed by AWS) and attached as 'Política de permissões' (Permission policy). An 'Editar' (Edit) button is located at the top right.

Resumo da política de permissões		
Nome da política	Tipo	Anexado como
AmazonS3ReadOnlyAccess	Gerenciadas pela AWS	Política de permissões
CloudWatchReadOnlyAccess	Gerenciadas pela AWS	Política de permissões

Resposta da pergunta: Uma role IAM é relevante pois ela pode ser configurada para dar ao usuário acesso a apenas o que ele vai precisar e as informações que ele precisa saber. Além de que só usuários com permissão podem modificar algo dos serviços.

5- Configuração de Alarmes no CloudWatch

Não soube fazer.