

AWS Academy Cloud Foundations (Fundamentos de nuvem da AWS Academy)

# Módulo 4: Segurança na Nuvem AWS



## Tópicos

- Modelo de responsabilidade compartilhada da AWS
- AWS Identity and Access Management (IAM)
- Proteção de novas contas da AWS
- Proteção de contas
- Proteção de dados na AWS
- Garantia da conformidade

## Atividades

- Atividade do modelo de responsabilidade compartilhada da AWS

## Demonstração

- Demonstração gravada do IAM

## Laboratório

- Introdução ao AWS IAM



## Teste de conhecimento

Depois de concluir este módulo, você deverá ser capaz de:

- Reconhecer o modelo de responsabilidade compartilhada
- Identificar a responsabilidade do cliente e a da AWS
- Reconhecer usuários, grupos e funções do IAM
- Descrever diferentes tipos de credenciais de segurança no IAM
- Identificar as etapas para a proteção de novas contas da AWS
- Explorar usuários e grupos do IAM
- Reconhecer como proteger dados da AWS
- Reconhecer programas de conformidade da AWS

## Módulo 4: Segurança na Nuvem AWS

# Seção 1: Modelo de responsabilidade compartilhada da AWS

# Modelo de responsabilidade compartilhada da AWS

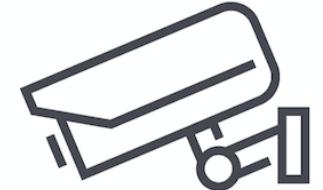


# Responsabilidade da AWS: segurança *da nuvem*

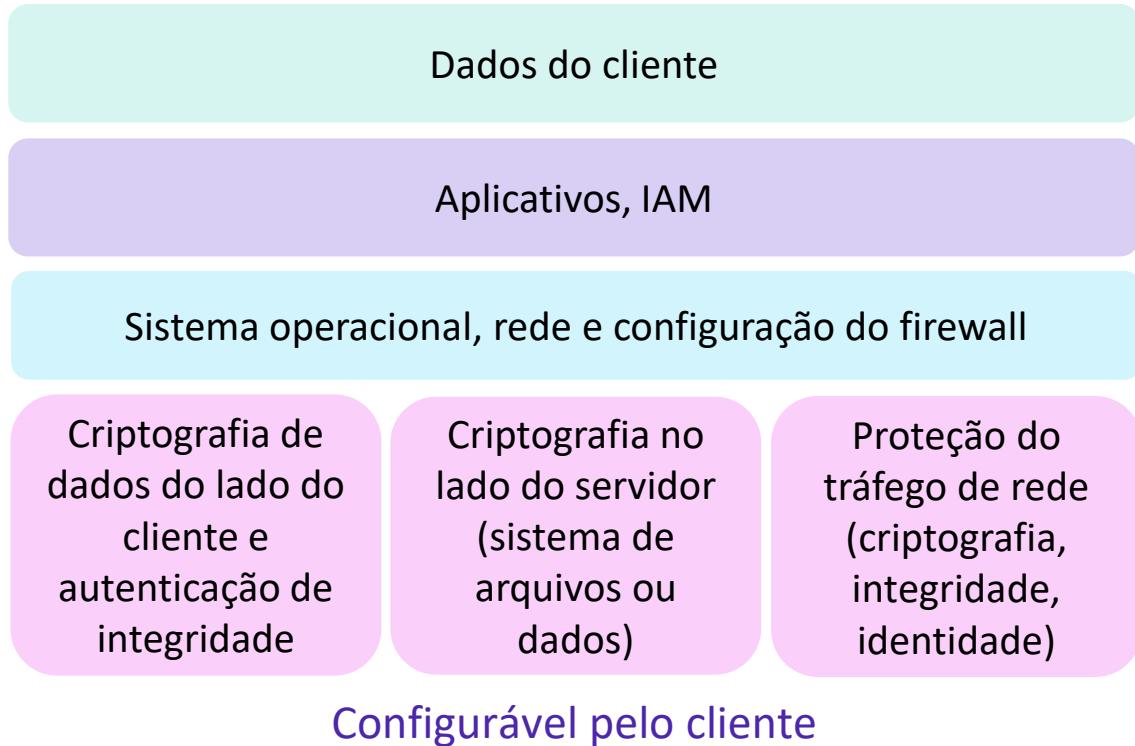


## Responsabilidades da AWS:

- Segurança física dos datacenters
  - Acesso controlado e baseado em necessidades
- Infraestrutura de hardware e software
  - Desativação de armazenamento, registro em log de acesso ao sistema operacional (SO) do host e auditoria
- Infraestrutura de rede
  - Detecção de intrusão
- Infraestrutura de virtualização
  - Isolamento de instância



# Responsabilidade do cliente: segurança na nuvem



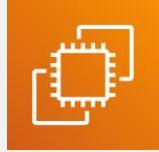
## Responsabilidades do cliente:

- **Sistema operacional** da instância do Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluindo aplicação de patches, manutenção
- **Aplicações**
  - Senhas, acesso baseado em função etc.
- **Configuração do grupo de segurança**
- **Firewalls** baseados em host ou SO
  - Incluindo sistemas de prevenção ou detecção de intrusão
- **Configurações de rede**
- **Gerenciamento de contas**
  - Configurações de permissão e login para cada usuário

# Características do serviço e responsabilidade de segurança



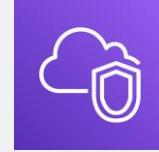
## Serviços de exemplo gerenciados pelo cliente



Amazon EC2



Amazon Elastic  
Block Store  
(Amazon EBS)



Amazon Virtual Private  
Cloud (Amazon VPC)

## Infraestrutura como um serviço (IaaS)

- O cliente tem mais flexibilidade em relação à configuração de rede e armazenamento
- O cliente é responsável por gerenciar mais aspectos da segurança
- O cliente configura os controles de acesso

## Serviços de exemplo gerenciados pela AWS



AWS Lambda



Amazon Relational  
Database Service  
(Amazon RDS)



AWS Elastic  
Beanstalk

## Plataforma como serviço (PaaS)

- O cliente não precisa gerenciar a infraestrutura subjacente
- A AWS gerencia o sistema operacional, a aplicação de patches de banco de dados, a configuração de firewall e a recuperação de desastres
- O cliente pode se concentrar no gerenciamento de código ou dados

# Características do serviço e responsabilidade de segurança (continuação)



## Exemplos de SaaS



AWS Trusted  
Advisor



AWS Shield



Amazon Chime

## Software como serviço (SaaS)

- O software é hospedado de maneira centralizada
- Licenciado em um modelo de assinatura ou pagamento conforme o uso.
- Os serviços normalmente são acessados por meio de um navegador da Web, um aplicativo móvel ou uma interface de programação de aplicativos (API)
- Os clientes não precisam gerenciar a infraestrutura que oferece suporte ao serviço

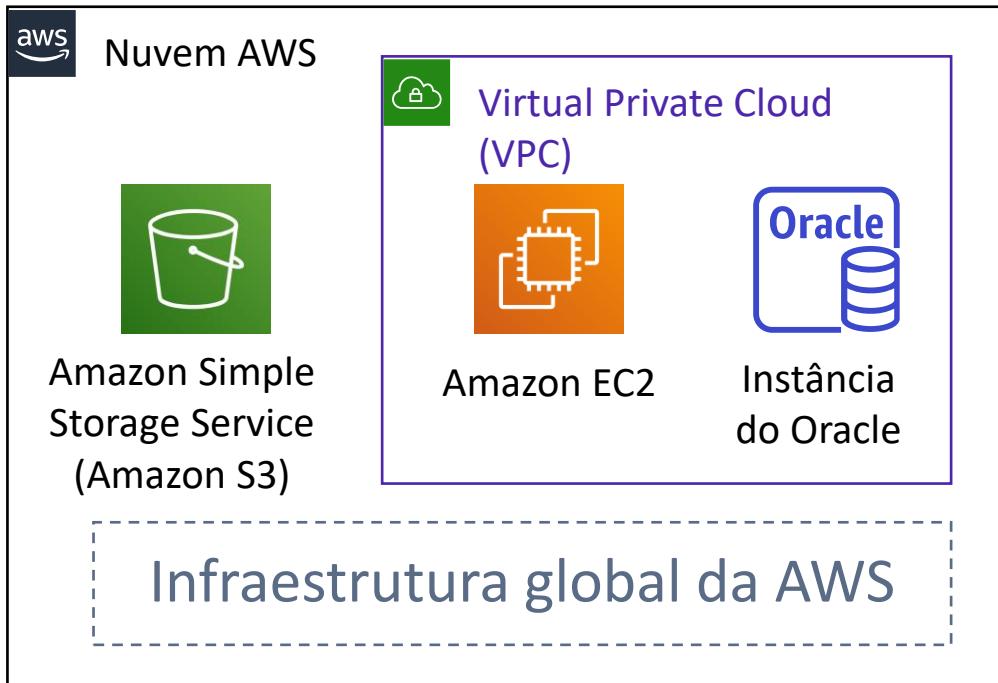
## Atividade: modelo de responsabilidade compartilhada da AWS



Foto de Pixabay da Pexels.

# Atividade: cenário 1 de 2

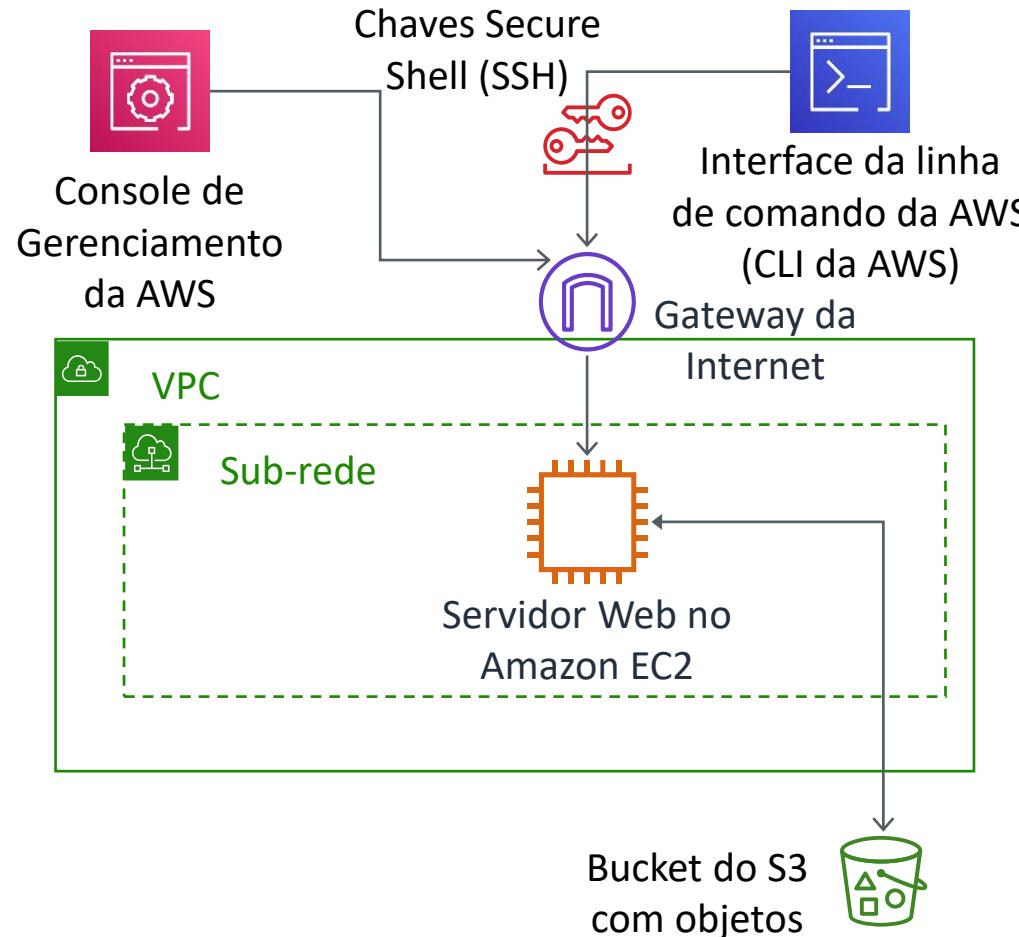
## Considerate esta implantação. Quem é responsável, a AWS ou o cliente?



1. Atualizações e patches para o sistema operacional na instância do EC2?
  - **RESPOSTA:** o cliente
2. Segurança física do datacenter?
  - **RESPOSTA:** AWS
3. Infraestrutura de virtualização?
  - **RESPOSTA:** AWS
4. Configurações do grupo de segurança do EC2?
  - **RESPOSTA:** o cliente
5. Configuração de aplicativos que são executados na instância do EC2?
  - **RESPOSTA:** o cliente
6. Atualizações ou patches do Oracle se a instância do Oracle for executada como uma instância do Amazon RDS?
  - **RESPOSTA:** AWS
7. Atualizações ou patches do Oracle se o Oracle for executado em uma instância do EC2?
  - **RESPOSTA:** o cliente
8. Configuração de acesso ao bucket do S3?
  - **RESPOSTA:** o cliente

# Atividade: cenário 2 de 2

## Considerate esta implantação. Quem é responsável, a AWS ou o cliente?



1. Garantir que o Console de Gerenciamento da AWS não seja invadido?
  - **RESPOSTA: AWS**
2. Configurar a sub-rede?
  - **RESPOSTA: o cliente**
3. Configurar a VPC?
  - **RESPOSTA: o cliente**
4. Proteger contra interrupções de rede nas regiões da AWS?
  - **RESPOSTA: AWS**
5. Proteger as chaves SSH?
  - **RESPOSTA: o cliente**
6. Garantir o isolamento de rede entre os dados dos clientes da AWS?
  - **RESPOSTA: AWS**
7. Garantir uma conexão de rede de baixa latência entre o servidor Web e o bucket do S3?
  - **RESPOSTA: AWS**
8. Importar a Multi-Factor Authentication para todos os logins de usuário?
  - **RESPOSTA: o cliente**

# Principais lições da Seção 1

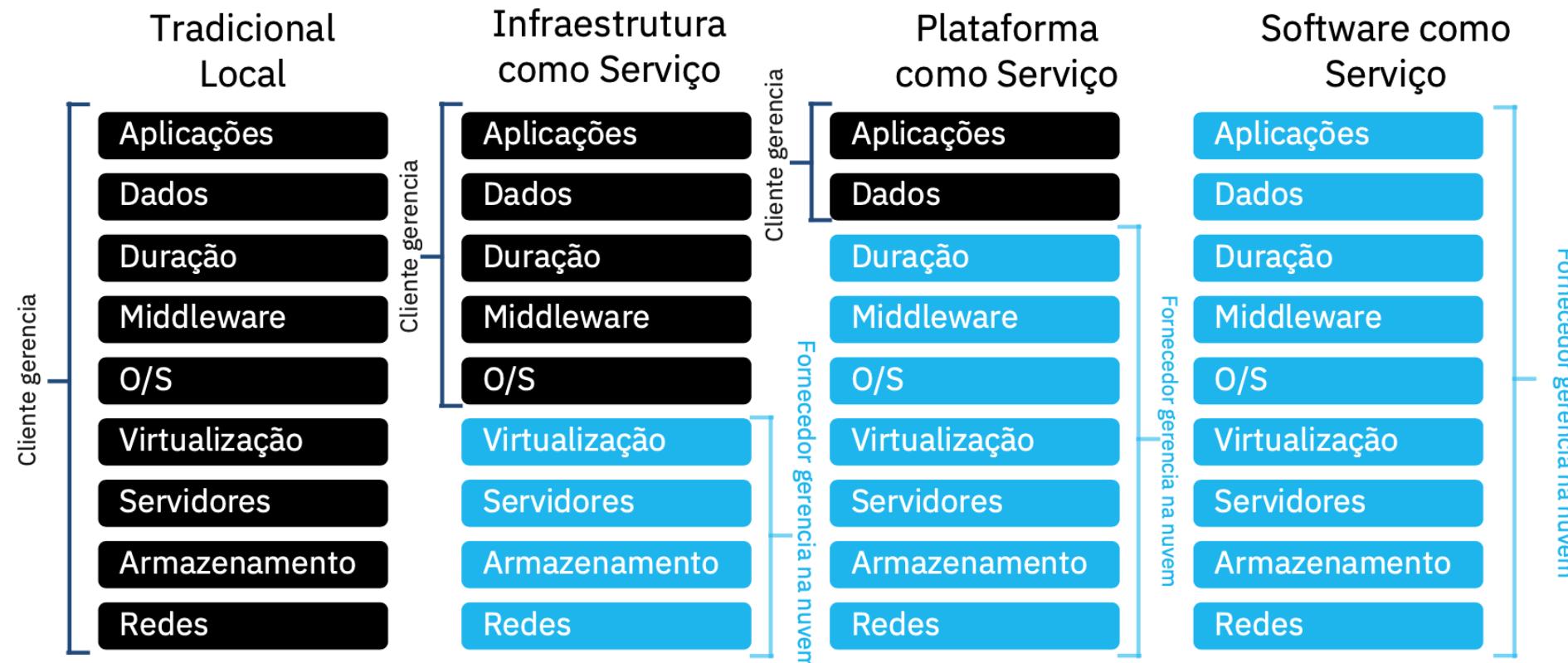


- A AWS e o cliente compartilham responsabilidades de segurança:
  - A AWS é responsável pela segurança **da** nuvem
  - O cliente é responsável pela segurança **na** nuvem
- **A AWS é responsável por proteger a infraestrutura** que executa os serviços de nuvem AWS, incluindo hardware, software, redes e instalações
- Para serviços categorizados como infraestrutura como serviço (IaaS), o **cliente é responsável por executar as tarefas necessárias de configuração e gerenciamento de segurança**
  - Por exemplo, configurações do grupo de segurança, firewall e patches de segurança e atualizações de sistema operacional convidado

Módulo 4: Segurança na Nuvem AWS

## Seção 2: AWS Identity and Access Management (IAM)

# Modelos de serviços em nuvem

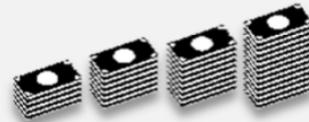


Customização; custo mais alto; mais lento para valorizar

Padronização; custo mais baixo; mais rápido para valorizar

# Oportunidades de segurança em nuvem

## Ataques sofisticados



Custo médio  
de brechas nos EUA

Mais de  
**US\$ 7 milhões**

## Mudança sem precedentes



**70%**

de executivos de segurança  
estão preocupados com a  
segurança de nuvem & mobile<sup>2</sup>

## Práticas insustentáveis

**85**



Ferramentas de

**45**



fornecedores

## Reputações sofrendo danos



**61%**

das organizações dizem que o  
roubo de dados e crimes  
cibernéticos são as maiores  
ameaças à sua reputação

## Crescimento de malwares móveis!

**614%**



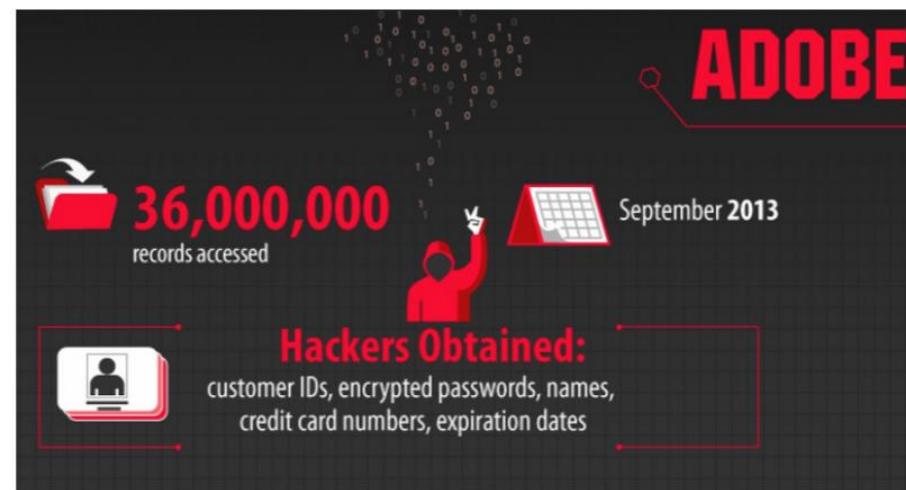
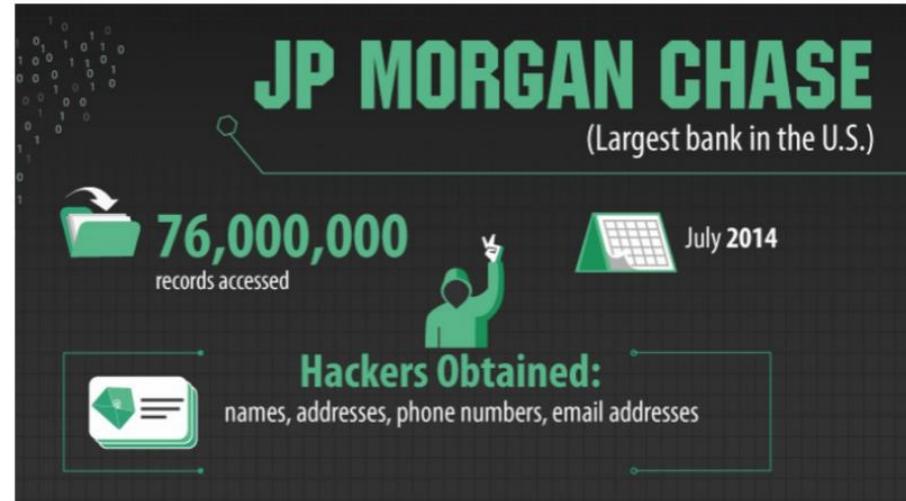
## Falta de habilidades em segurança



**83%**

das empresas têm dificuldade  
em encontrar as habilidades  
de segurança que precisam

# Mas há significativas violações recentes de dados



Fonte: <http://visual.ly/confidential-top-11-worst-data-breaches-all-time>

# 80%

dos executivos senior de TI disseram que planejam armazenar dados em novos ambientes de tecnologia, como a nuvem<sup>1</sup>

**Desses, 85% estavam  
"preocupados" ou "muito  
preocupados" com a  
segurança na nuvem<sup>1</sup>**

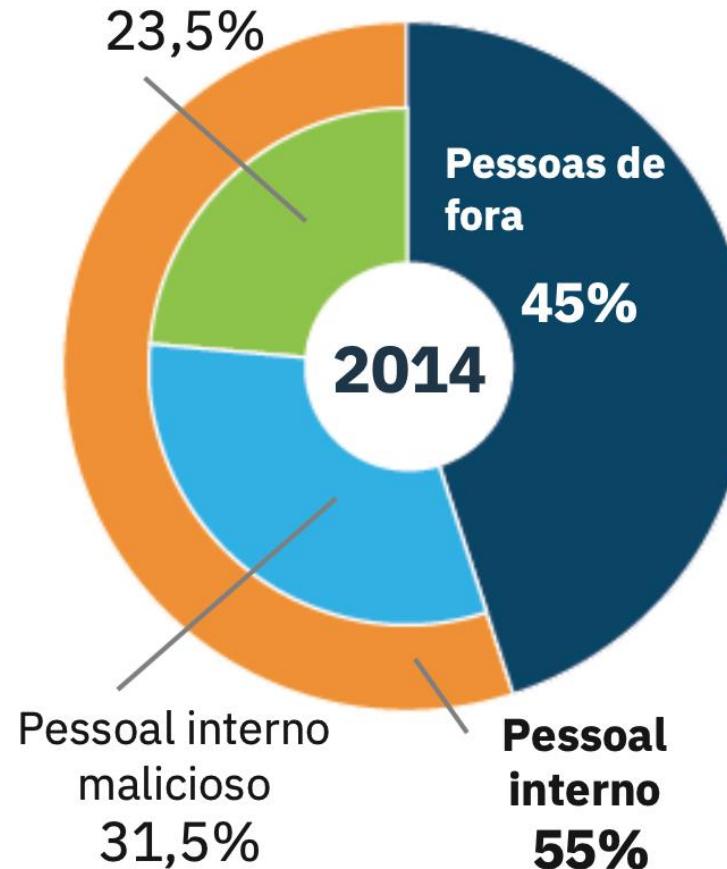


<sup>1</sup> [Vormetric 2016 Cloud Adoption Report](#)

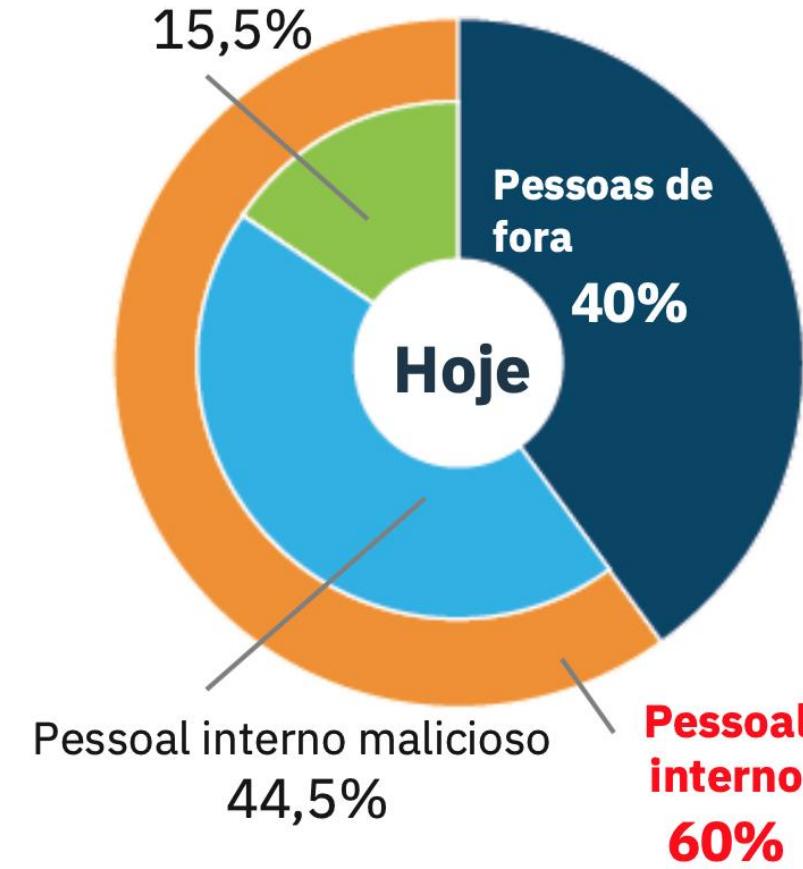
# O cenário em expansão para a nuvem abre novas portas para ameaças

Por que você deve se preocupar?

Atores inadvertidos



Atores inadvertidos

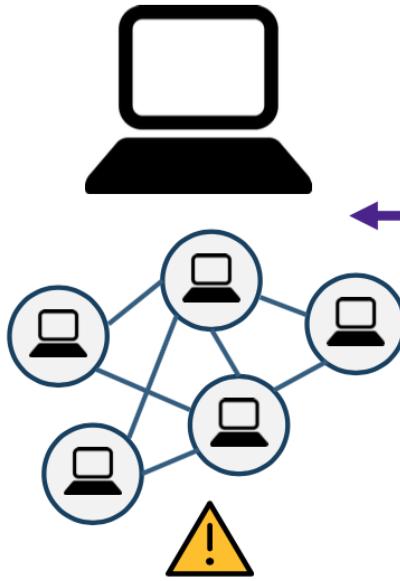


# Onde os ataques ocorrem normalmente?

VETORES DE ATAQUE

y

## No local



- 1 Acesso não autorizado via rede interna

## Externamente (a caminho da nuvem)

- 3 Acesso hackeado (via phishing, por exemplo)
- 2 O tráfego entre o cliente e o site em nuvem pode ser lido. Por exemplo: dados não criptografados para um ambiente de teste

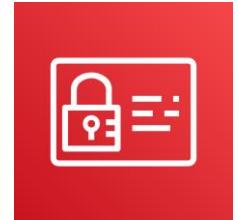
## Nuvem

- 4 Ameaças à segurança física:
  - Roubo de servidor
  - Incêndios, enchentes
- 5 Arquivos com vírus enviados para a nuvem
- 6 Dados serem lidos quando trocados entre aplicações na nuvem
- 7 Dados serem acessados por:
  - pessoas fora da aplicação em nuvem
  - outros locatários da mesma aplicação em nuvem
  - o provedor da aplicação em nuvem

# AWS Identity and Access Management (IAM)



- Use o **IAM** para gerenciar o acesso aos **recursos da AWS** –
  - Um recurso é uma entidade em uma conta da AWS com a qual você pode trabalhar
  - Exemplo de recursos: uma instância do Amazon EC2 ou um bucket do Amazon S3
- *Exemplo:* controle quem pode encerrar instâncias do Amazon EC2
- Defina direitos de acesso refinados –
  - **Quem** pode acessar o recurso
  - **Quais** recursos podem ser acessados e o que o usuário pode fazer com o recurso
  - **Como** os recursos podem ser acessados
- O IAM é um recurso de conta da AWS gratuito



AWS Identity and Access Management (IAM)

# IAM: componentes essenciais



Usuário do IAM

Uma **pessoa** ou **aplicativo** que pode se autenticar com uma conta da AWS.



Grupo do IAM

Uma **coleção de usuários do IAM** que recebem autorização idêntica.



Política do IAM

O documento que define **quais recursos podem ser acessados** e o **nível de acesso** a cada recurso.



Função do IAM

Mecanismo útil para conceder um conjunto de permissões para fazer solicitações de serviço da AWS.

# Autenticar como um usuário do IAM para obter acesso



Ao definir um **usuário do IAM**, você seleciona **os tipos de acesso** que o usuário tem permissão para usar.

- **Acesso programático**

- Autentique usando:
  - ID da chave de acesso
  - Chave de acesso secreta
- Fornece acesso à CLI e ao SDK da AWS



CLI da AWS



Ferramentas e  
SDKs da AWS

- **Acesso ao Console de Gerenciamento da AWS**

- Autentique usando:
  - ID *ou* alias da conta com 12 dígitos
  - Nome de usuário do IAM
  - Senha do IAM
- Se ativada, a **Multi-Factor Authentication (MFA)** solicita um código de autenticação.



Console de  
Gerenciamento da AWS

- A MFA oferece maior segurança.
- Além do nome de usuário e da senha, a MFA requer um código de autenticação exclusivo para acessar os serviços da AWS.

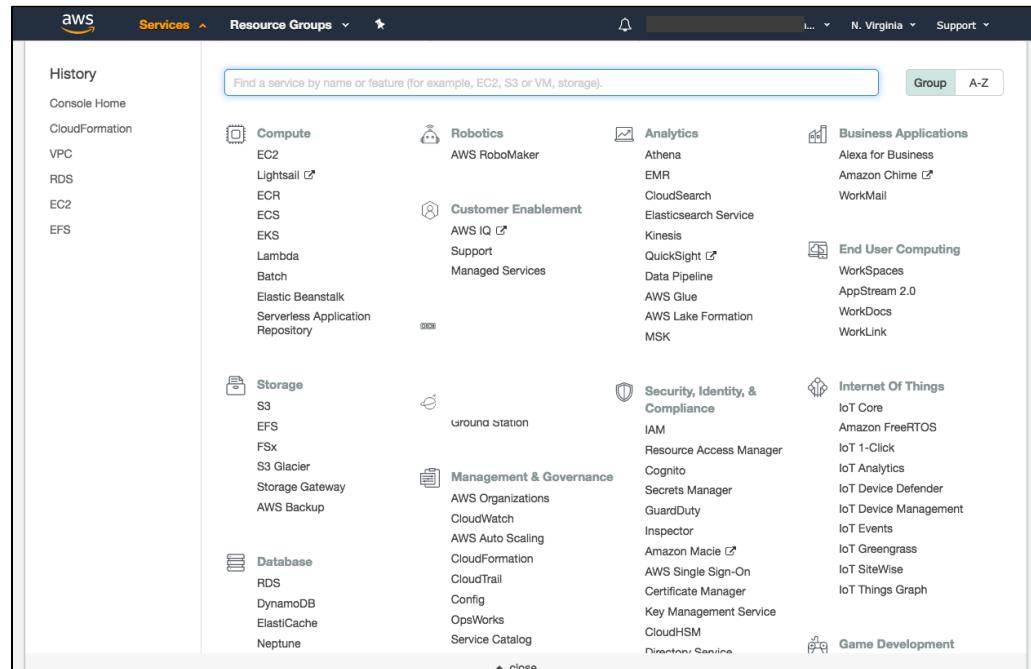
Account: [REDACTED]

User Name: [REDACTED]

Password: [REDACTED]

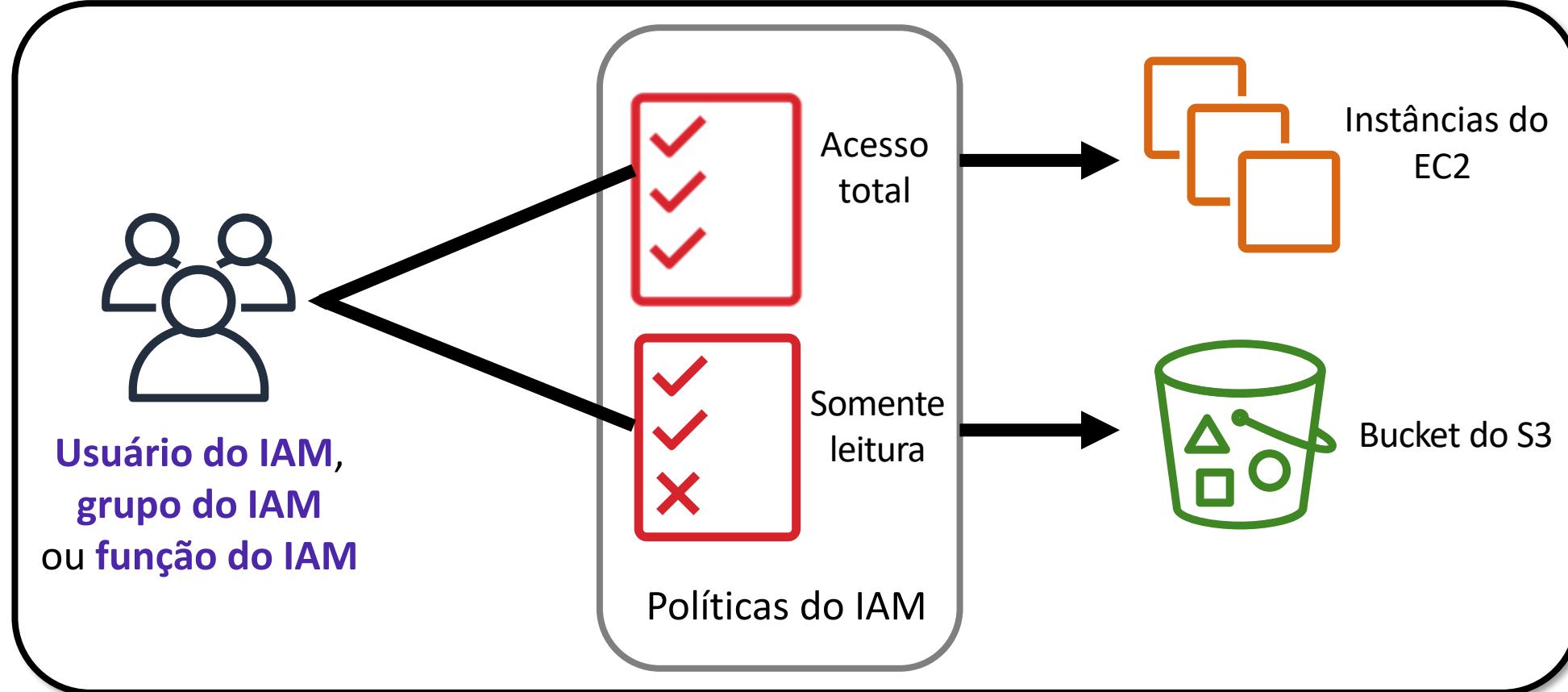
MFA users, enter your code on the next screen.

Sign In



# Autorização: quais ações são permitidas

*Depois que o usuário ou o aplicativo estiver conectado à conta da AWS, o que ele poderá fazer?*



- Atribua permissões criando uma política do IAM.
- As permissões determinam **quais recursos e operações** são permitidos:
  - Todas as permissões são implicitamente negadas por padrão.
  - Se algo for explicitamente negado, nunca será permitido.

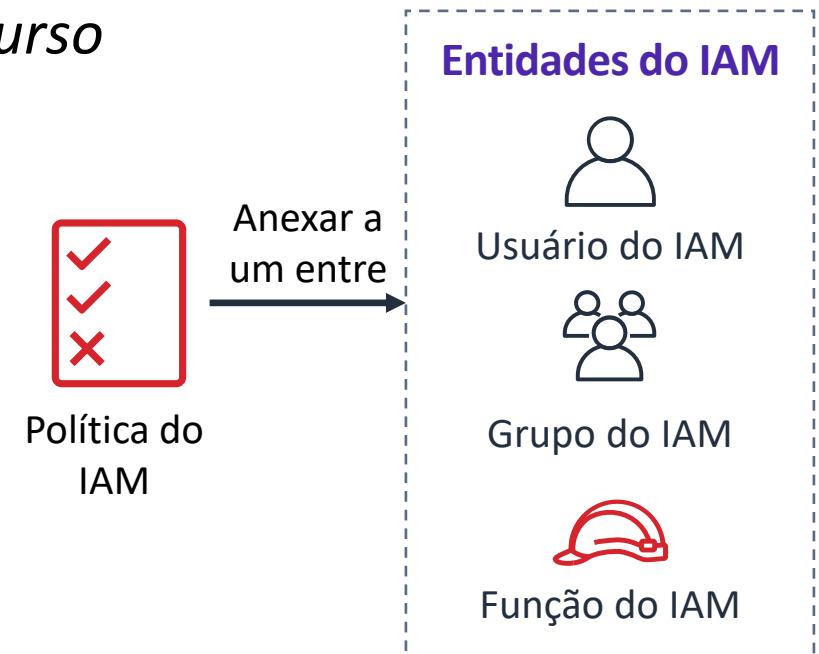
**Prática recomendada:** siga o **princípio do privilégio mínimo**.



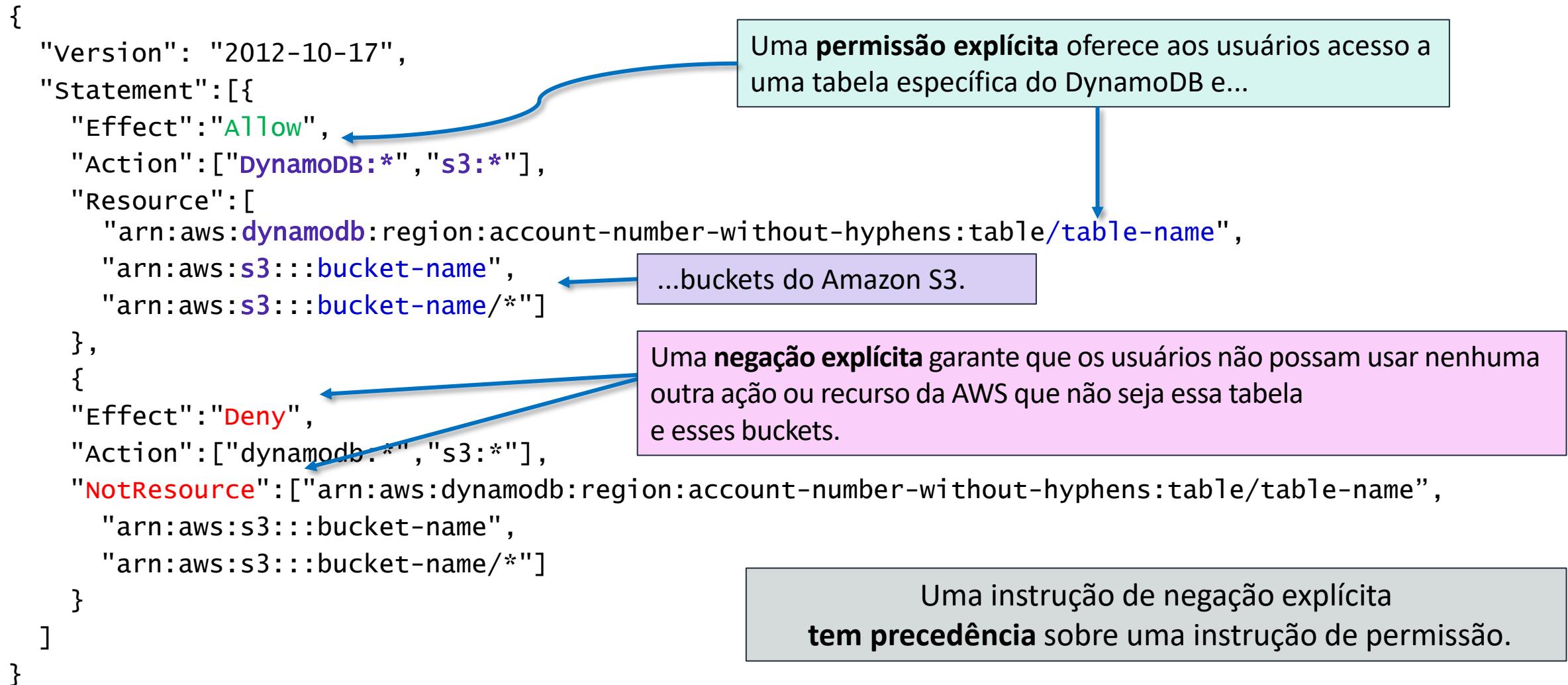
Permissões do IAM

Observação: o escopo das configurações de serviço do IAM é **global**. As configurações se aplicam a todas as regiões da AWS.

- Uma política do IAM é um documento que define permissões
  - Habilita um controle de acesso refinado
- Dois tipos de políticas: *baseadas em identidade e em recurso*
- Políticas **baseadas em identidade** –
  - Anexe uma política a qualquer entidade do IAM
    - Um **usuário do IAM**, um **grupo do IAM** ou uma **função do IAM**
  - As políticas especificam:
    - Ações que ***podem*** ser executadas pela entidade
    - Ações que ***não podem*** ser executadas pela entidade
  - Uma única *política* pode ser anexada a várias *entidades*
  - Uma única *entidade* pode ter várias *políticas* anexadas a ela
- Políticas **baseadas em recursos**
  - Anexadas a um recurso (como um bucket do S3)



# Exemplo de política do IAM



# Exemplo de política



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:Describe*",  
      "Resource": "*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": "elasticloadbalancing:Describe*",  
      "Resource": "*"  
    },  
  ]  
}
```

Uma política define quais ações são permitidas ou negadas para recursos específicos da AWS. Esta política concede permissão para listar e descrever informações sobre EC2 e Elastic Load Balancing. Essa capacidade de visualizar recursos, mas não os modificar, é ideal para atribuir a uma role (função) de suporte.

# Exemplo de política



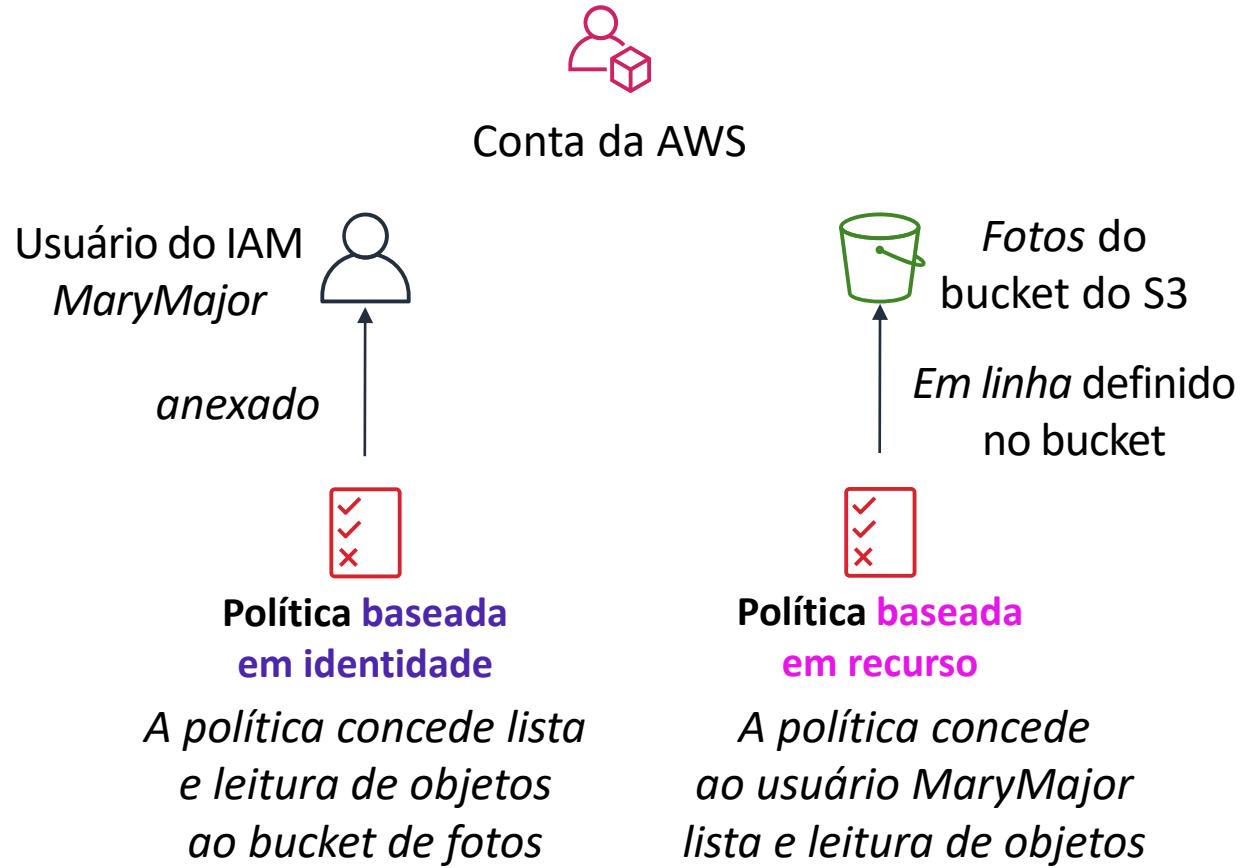
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:Describe*",  
      "Resource": "*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": "elasticloadbalancing:Describe*",  
      "Resource": "*"  
    },  
  ]  
}
```

A estrutura básica das instruções em uma política do IAM é:

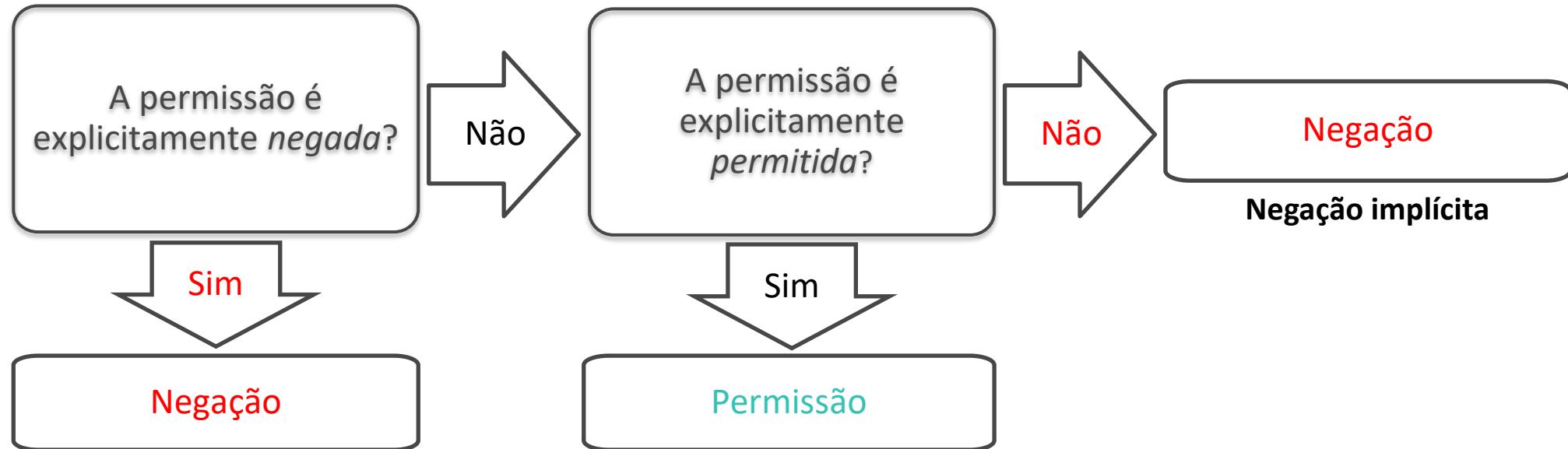
- **Effect (Efeito)** indica se deseja Allow (Permitir) ou Deny (Negar) as permissões.
- **Action (Ação)** especifica as chamadas de API que podem ser feitas em um serviço da AWS (por exemplo, ec2:Describe\*).
- **Resource (Recurso)** define o escopo das entidades cobertas pela regra de política (por exemplo, um bucket específico do Amazon S3 ou uma instância Amazon EC2; ou \*, que significa qualquer recurso).

# Políticas baseadas em recursos

- As *políticas baseadas em identidade* são anexadas a um usuário, um grupo ou uma função
- **As políticas baseadas em recursos** são anexadas a um recurso (*não* a um usuário, um grupo ou uma função)
- Características das políticas baseadas em recursos –
  - Especificam quem tem acesso ao recurso e quais ações podem ser executadas nele
  - As políticas são apenas *em linha*, não gerenciadas
- As políticas baseadas em recursos são compatíveis apenas com alguns serviços da AWS

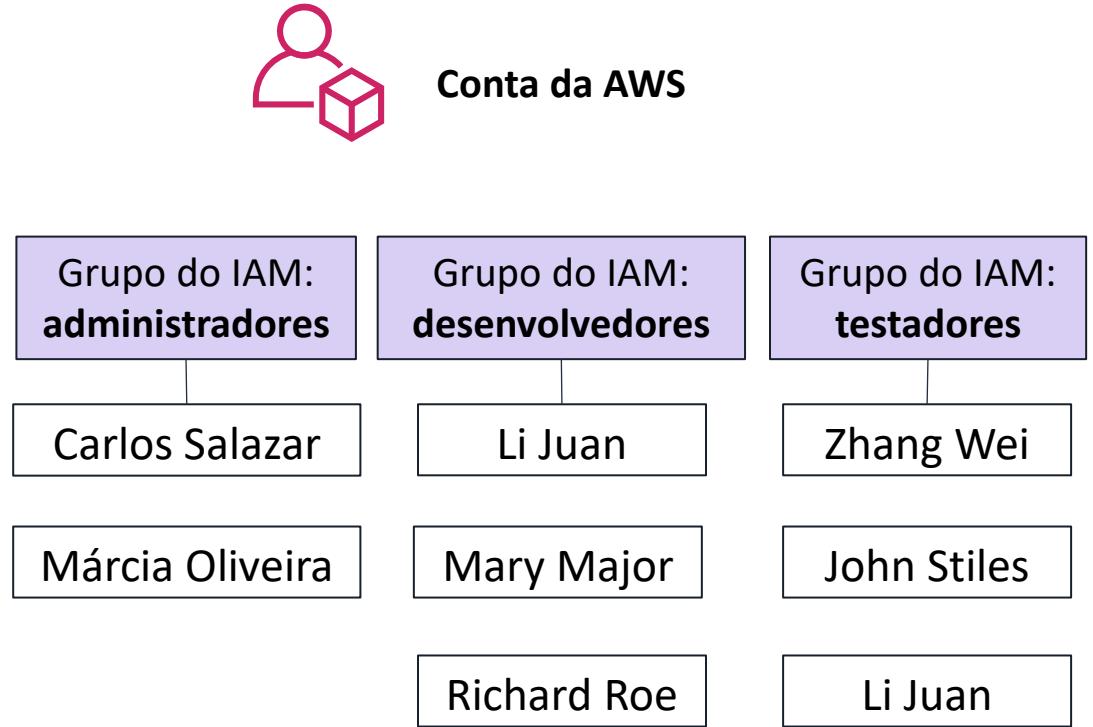


Como o IAM determina permissões:



# Grupos do IAM

- Um **grupo do IAM** é um conjunto de usuários do IAM
- Um grupo é usado para conceder as mesmas permissões a vários usuários
  - Permissões concedidas ao anexar *política* ou políticas do IAM ao grupo
- Um usuário pode pertencer a vários grupos
- Não há grupo padrão
- Os grupos não podem ser aninhados



- Uma **função do IAM** é uma identidade do IAM com permissões específicas
- Semelhante a um usuário do IAM
  - Anexe políticas de permissões a ela
- Diferente de um usuário do IAM
  - Não associada exclusivamente a uma pessoa
  - Destinada a ser *assumida* por uma **pessoa**, um **aplicativo** ou um **serviço**
- A função fornece credenciais de segurança *temporárias*
- Exemplos de como as funções do IAM são usadas para **delegar** acesso –
  - Usada por um usuário do IAM na mesma conta da AWS que a função
  - Usada por um serviço da AWS, como o Amazon EC2, na mesma conta que a função
  - Usada por um usuário do IAM em uma conta da AWS diferente da função



Função do IAM

# Exemplo de uso de uma função do IAM

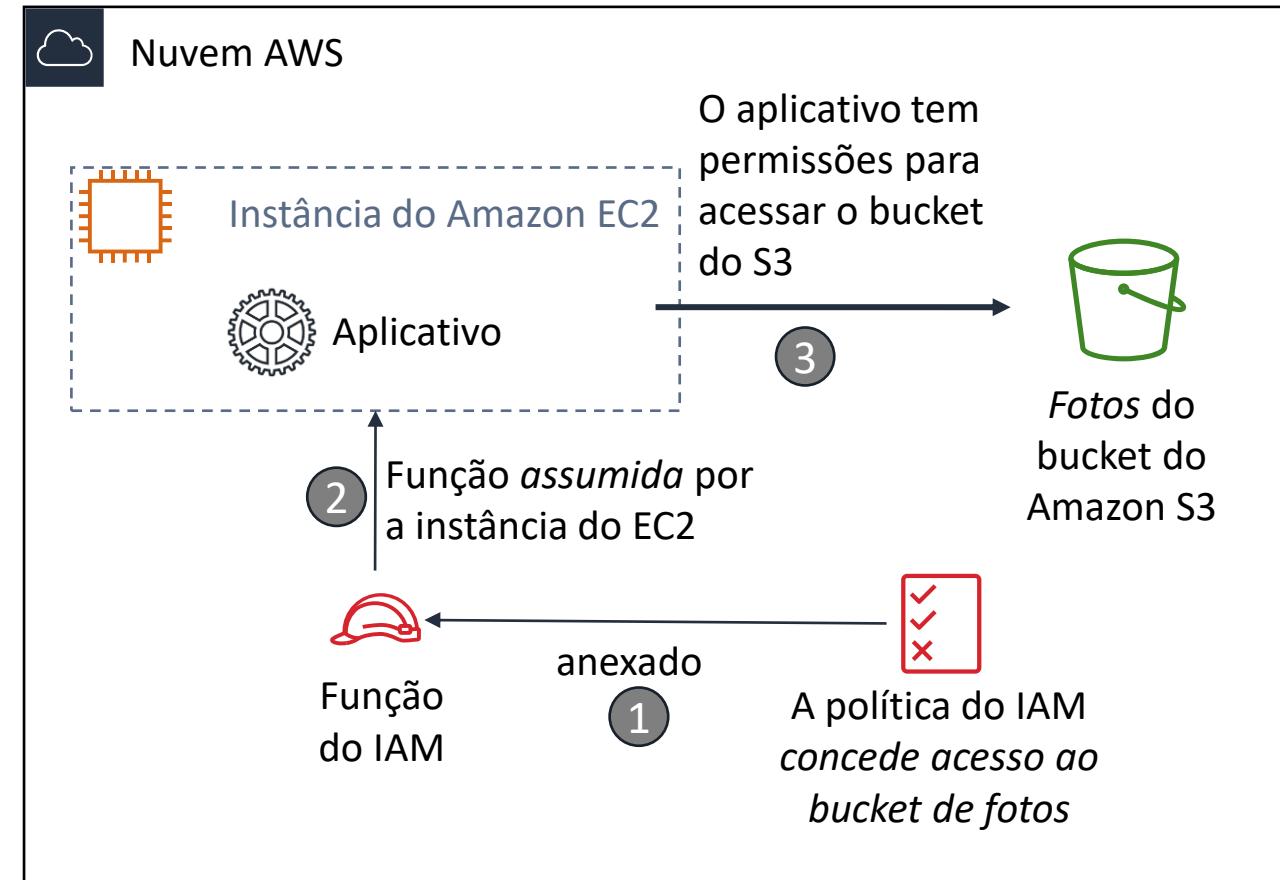


## Cenário:

- Um aplicativo executado em uma instância do EC2 precisa de acesso a um bucket do S3

## Solução:

- Defina uma política do IAM que conceda acesso ao bucket do S3.
- Anexe a política a uma função
- Permita que a instância do EC2 assuma a função



# Principais lições da Seção 2



- As **políticas do IAM** são criadas com JavaScript Object Notation (JSON) e definem permissões.
  - As políticas do IAM podem ser anexadas a qualquer **entidade do IAM**.
  - As entidades são usuários do IAM, grupos do IAM e funções do IAM.
- Um **usuário do IAM** fornece uma maneira para uma pessoa, um aplicativo ou um serviço se autenticar na AWS.
- Um **grupo do IAM** é uma maneira simples de anexar as mesmas políticas a vários usuários.
- Uma **função do IAM** pode ter políticas de permissões anexadas a ela e ser usada para delegar acesso temporário a usuários ou aplicativos.

# Demonstração gravada: IAM



**Configurar demonstração**

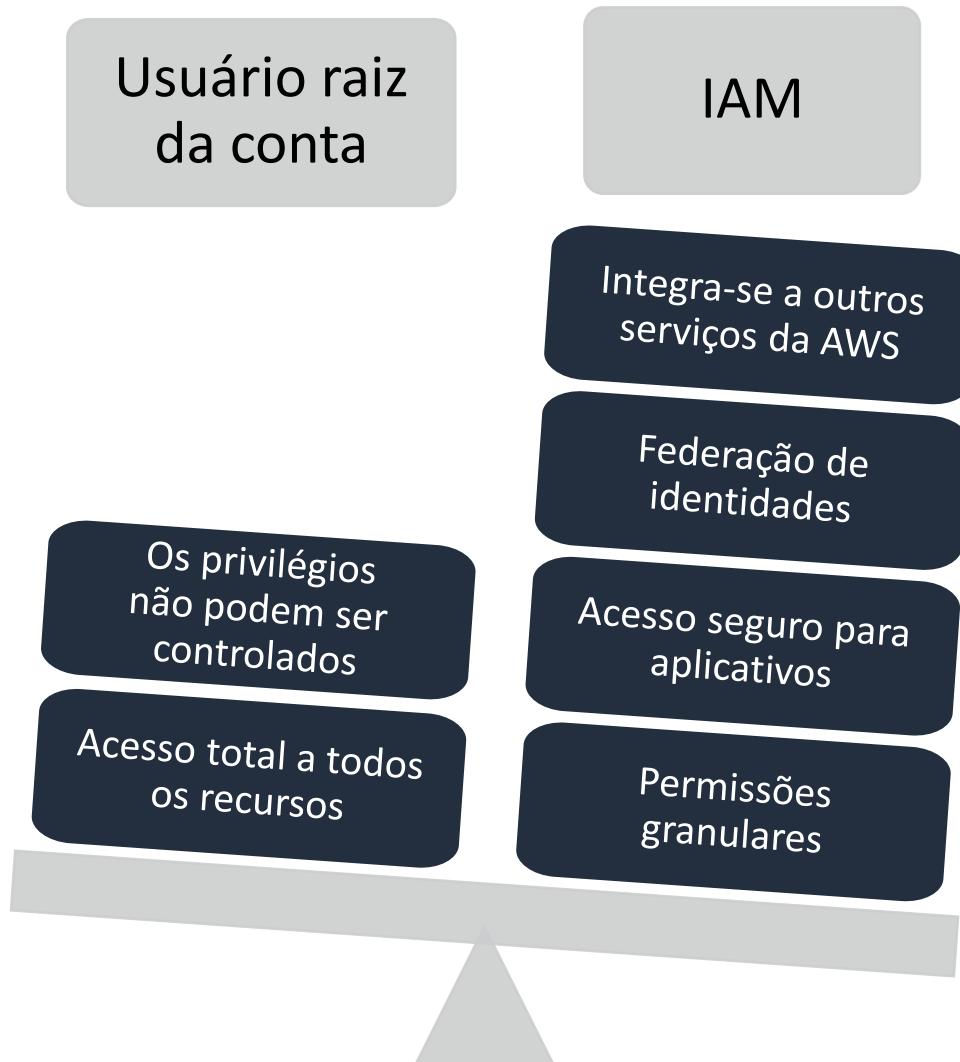
AWS Identity and Access Management (IAM)

A dark blue rectangular area containing the title and subtitle, with a faint wireframe cube pattern visible in the background.

Módulo 4: Segurança na Nuvem AWS

# Seção 3: Proteção de uma nova conta da AWS

# Acesso de usuário raiz da conta da AWS em comparação ao acesso do IAM



- **Prática recomendada:** **não use o usuário raiz da conta da AWS, exceto quando necessário.**
  - O acesso ao **usuário raiz da conta** requer o login com o *endereço de e-mail* (e a senha) que você usou para criar a conta.
  - Ações de exemplo que só podem ser realizadas com o usuário raiz da conta:
    - Atualizar a senha do usuário raiz da conta
    - Alterar o plano do AWS Support
    - Restaurar as permissões de um usuário do IAM
    - Alterar as configurações da conta (por exemplo, informações de contato, regiões permitidas)

# Proteção de novas contas da AWS: usuário raiz da conta



## Etapa 1: Parar de usar o usuário raiz da conta o mais rápido possível.

- O usuário raiz da conta tem acesso irrestrito a todos os seus recursos.
- Para parar de usar o usuário raiz da conta:
  1. Enquanto estiver conectado como o usuário raiz da conta, **crie um usuário do IAM** para você mesmo. Salve as chaves de acesso, se necessário.
  2. Crie um grupo do IAM, atribua a ele permissões completas de administrador e adicione o usuário do IAM ao grupo.
  3. Desabilite e **remova as chaves de acesso do usuário raiz da conta**, se elas existirem.
  4. **Habilite uma política de senha** para usuários.
  5. Faça login com as novas credenciais de usuário do IAM.
  6. Armazene as credenciais de usuário raiz da sua conta em um local seguro.

## Etapa 2: Habilitar Multi-Factor Authentication (MFA)

- Exija MFA para o **usuário raiz da sua conta** e para **todos os usuários do IAM**.
- Você também pode usar a MFA para controlar o acesso às APIs de serviço da AWS.
- Opções para recuperar o token de MFA –
  - Aplicativos compatíveis com MFA virtual:
    - Google Authenticator.
    - Authy Authenticator (aplicativo Windows Phone).
  - Dispositivos de chave de segurança U2F:
    - Por exemplo, YubiKey.
  - Opções de MFA de hardware:
    - Chaveiro ou cartão de exibição oferecido pela [Gemalto](#).



Token de MFA

# Proteção de novas contas da AWS: AWS CloudTrail



## Etapa 3: Usar o AWS CloudTrail.

- O CloudTrail rastreia as atividades dos usuários em sua conta.
  - Ele registra todas as solicitações de API para recursos em todos os serviços compatíveis da sua conta.
- O histórico básico de eventos do AWS CloudTrail é habilitado por padrão e gratuito.
  - Ele contém todos os dados de eventos de gerenciamento nos últimos 90 dias de atividade da conta.
- Para acessar o CloudTrail –
  1. Faça login no **Console de Gerenciamento da AWS** e escolha o serviço **CloudTrail**.
  2. Clique em **Event history (Histórico de eventos)** para visualizar, filtrar e pesquisar os últimos 90 dias de eventos.
- **Para habilitar logs além de 90 dias e habilitar alertas de eventos especificados, crie uma trilha.**
  1. Na página CloudTrail Console trails (Trilhas do console do CloudTrail), clique em **Create trail (Criar trilha)**.
  2. Atribua um nome a ela, aplique-a a todas as regiões e crie um novo bucket do Amazon S3 para armazenamento de logs.
  3. Configure restrições de acesso no bucket do S3 (por exemplo, somente usuários admin devem ter acesso).

## Etapa 4: Habilitar um relatório de faturamento, como o relatório de custos e uso da AWS.

- Os relatórios de faturamento oferecem informações sobre o uso dos recursos da AWS e os custos estimados para esse uso.
- A AWS entrega os relatórios para o bucket do Amazon S3 que você especifica.
  - O relatório é atualizado pelo menos uma vez por dia.
- O **relatório de custos e uso da AWS** monitora seu uso da AWS e fornece cobranças estimadas associadas à sua conta da AWS por hora ou por dia.

## Módulo 4: Segurança na Nuvem AWS

Opcional: Proteção de novas contas  
da AWS – demonstração completa

# Análise do status de segurança do IAM

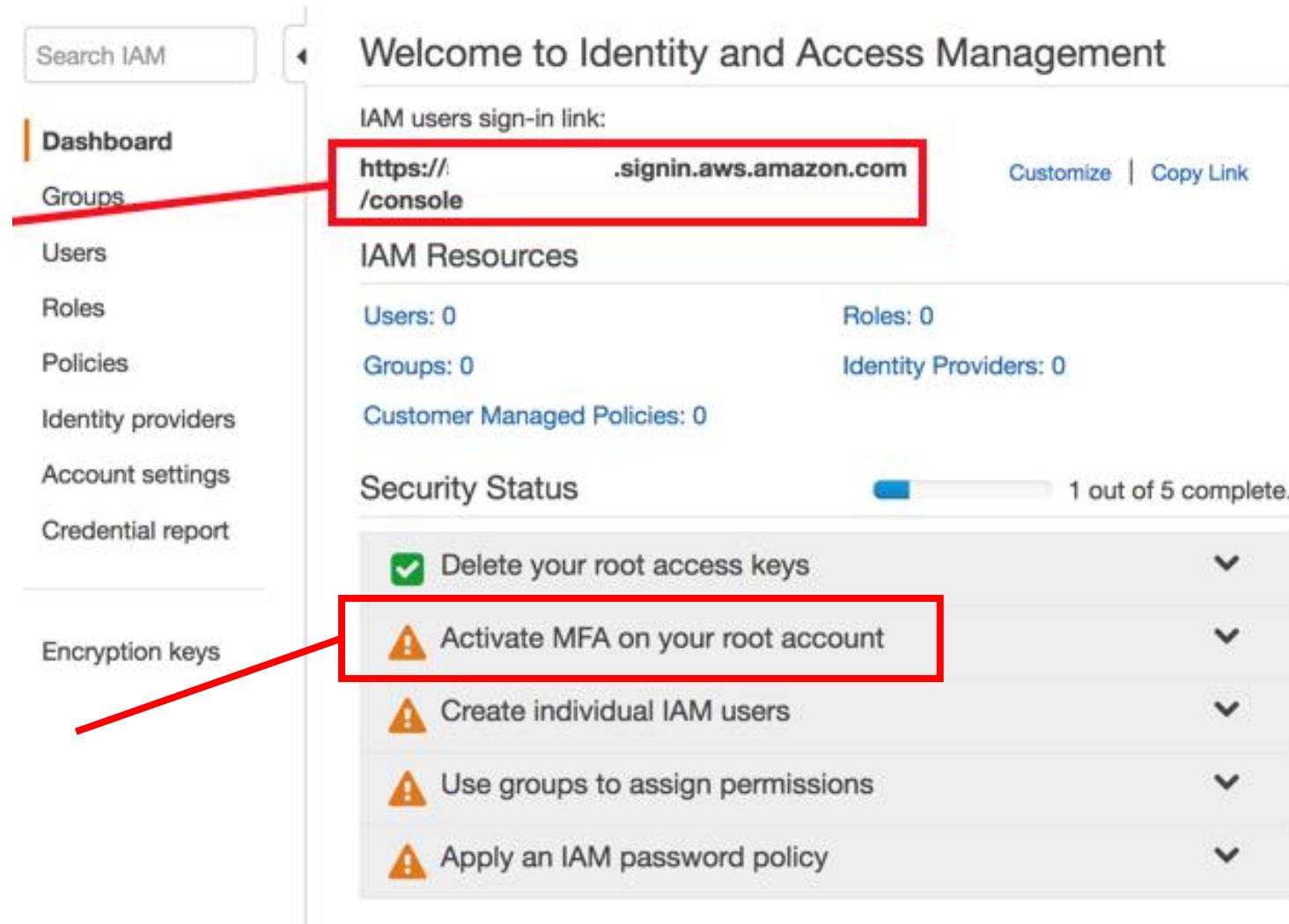


## Link de login personalizado

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with options like Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The 'Groups' option is highlighted with a red arrow pointing to it. The main area is titled 'Welcome to Identity and Access Management'. It features a 'IAM users sign-in link:' section with a URL: <https://signin.aws.amazon.com/console>. This URL is highlighted with a red box. Below this, there's a 'Customize' and 'Copy Link' button. The 'IAM Resources' section shows 0 users, 0 roles, 0 groups, 0 identity providers, and 0 customer managed policies. The 'Security Status' section indicates '1 out of 5 complete.' with a progress bar. Under 'Security Status', there are five items: 'Delete your root access keys' (checked), 'Activate MFA on your root account', 'Create individual IAM users', 'Use groups to assign permissions', and 'Apply an IAM password policy'. Each item has a dropdown arrow icon to its right.

# Ative a MFA no usuário raiz da conta

**Link de login  
personalizado**



Welcome to Identity and Access Management

IAM users sign-in link:  
<https://signin.aws.amazon.com/console>

Customize | Copy Link

**IAM Resources**

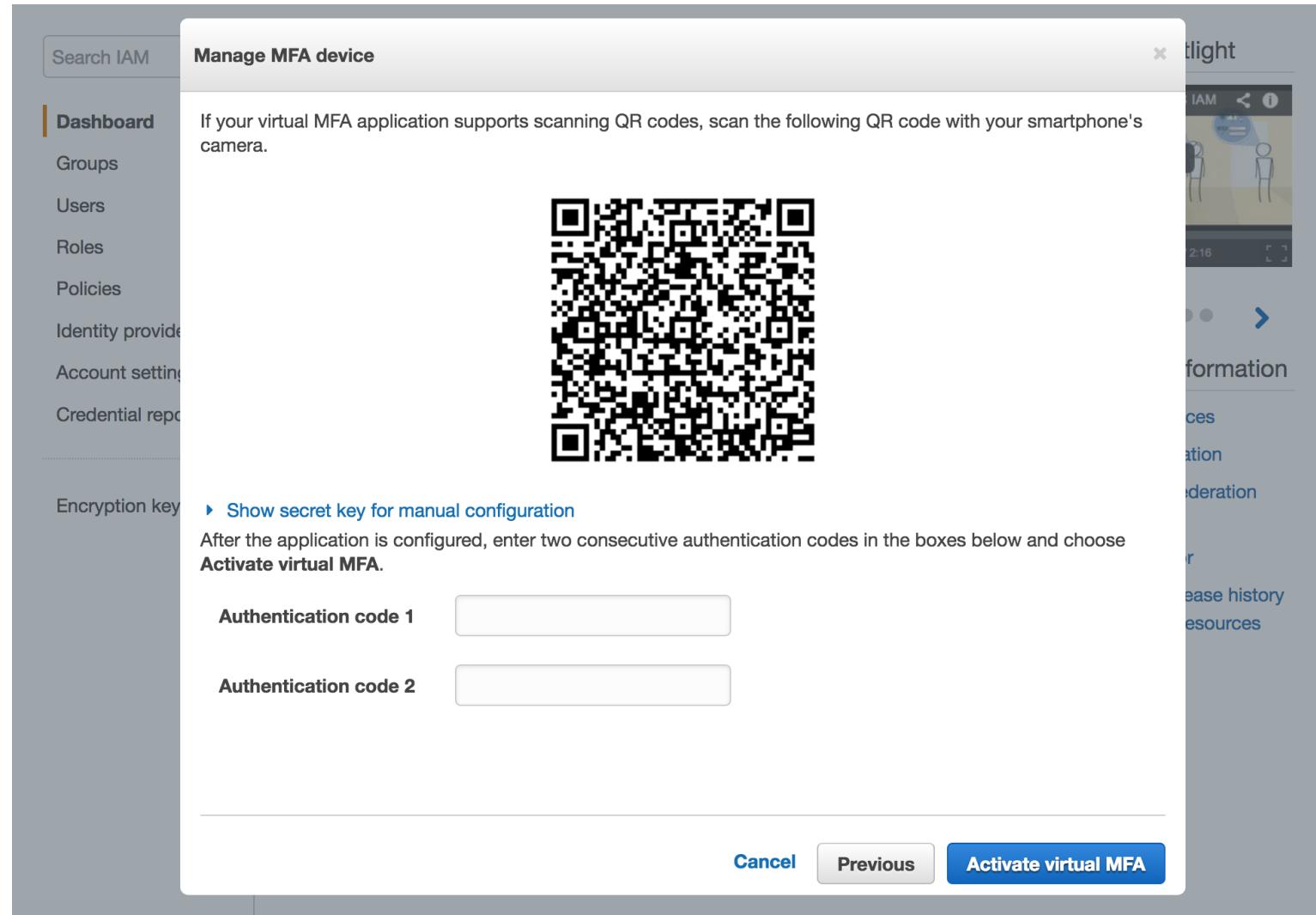
Users: 0	Roles: 0
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

**Security Status**  1 out of 5 complete.

- Delete your root access keys
-  **Activate MFA on your root account**
-  Create individual IAM users
-  Use groups to assign permissions
-  Apply an IAM password policy

Ativação da MFA

# Ative a MFA no usuário raiz da conta



# A MFA no usuário raiz da conta está ativada



Search IAM

**Dashboard**

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

---

Encryption keys

MFA ativada

Welcome to Identity and Access Management

IAM users sign-in link:  
<https://raysinut.signin.aws.amazon.com/console>    Customize | Copy Link

**IAM Resources**

Users: 0	Roles: 0
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

**Security Status** 2 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input checked="" type="checkbox"/> Activate MFA on your root account	▼
Create individual IAM users	▼
Use groups to assign permissions	▼
Apply an IAM password policy	▼

# Crie um usuário do IAM individual (1)



Search IAM

**Dashboard**

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

---

Encryption keys

**Criação de usuários do IAM**

Welcome to Identity and Access Management

IAM users sign-in link:  
<https://raysinut.signin.aws.amazon.com/console>      [Customize](#) | [Copy Link](#)

**IAM Resources**

Users: 0	Roles: 0
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

**Security Status** 2 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

# Crie um usuário do IAM individual (2)



## Add user



### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

Mic

[+ Add another user](#)

### Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*  **Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password\*  Autogenerated password

Custom password

Require password reset

User must create a new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

# Crie um usuário do IAM individual (3)



Add user

1

Details

2

Permissions

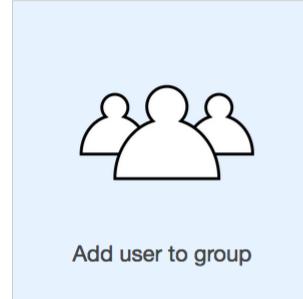
3

Review

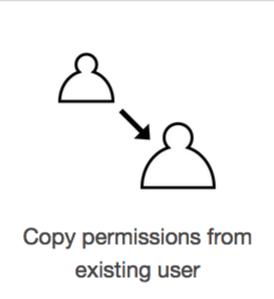
4

Complete

Set permissions for M



Add user to group



Copy permissions from  
existing user



Attach existing policies  
directly

## i Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

[Create group](#)

[Cancel](#)

[Previous](#)

[Next: Review](#)

# Crie um usuário do IAM individual (4)



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name Administrators

[Create policy](#) [Refresh](#)

	Policy name	Type	Attachments	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to relat...
<input type="checkbox"/>	AlexaForBusinessGatewayEx...	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessReadOnlyA...	AWS managed	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdminist...	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gatew...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFu...	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToC...	AWS managed	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Managemen...
<input type="checkbox"/>	AmazonAppStreamReadOnly...	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Mana...

Showing 313 results

[Cancel](#) [Create group](#)

# Crie um usuário do IAM individual (5)



Add user

Set permissions for M

1 Details    2 Permissions    3 Review    4 Complete

**Permissions**

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Create group Refresh

Group	Attached policies
Administrators	AdministratorAccess

Showing 1 result

Cancel Previous Next: Review

# Criação de usuário do IAM bem-sucedida



Add user

1

Details

2

Permissions

3

Review

4

Complete

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://raysia.sigin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
	Mi...	AKI...	***** Show	***** Show	<input checked="" type="checkbox"/> Send email

Close

# Status de segurança do painel do IAM



Search IAM

**Dashboard**

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

**Criação da política de senha**

Welcome to Identity and Access Management

IAM users sign-in link:  
<https://raysinut.signin.aws.amazon.com/console>

Customize | Copy Link

**IAM Resources**

Users: 1      Roles: 0

Groups: 1      Identity Providers: 0

Customer Managed Policies: 0

**Security Status** 4 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input checked="" type="checkbox"/> Activate MFA on your root account	▼
<input checked="" type="checkbox"/> Create individual IAM users	▼
<input checked="" type="checkbox"/> Use groups to assign permissions	▼
<b>⚠ Apply an IAM password policy</b>	▼

# Defina uma política de senhas do IAM



Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

**Account settings**

Credential report

Encryption keys

**Password Policy**

You have unsaved changes to your password policy.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

Require at least one uppercase letter i

Require at least one lowercase letter i

Require at least one number i

Require at least one non-alphanumeric character i

Allow users to change their own password i

Enable password expiration i

Password expiration period (in days):

Prevent password reuse i

Number of passwords to remember:

Password expiration requires administrator reset i

**Apply password policy** **Delete password policy**

# Verificações de status de segurança concluídas



Search IAM

**Dashboard**

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Welcome to Identity and Access Management

IAM users sign-in link:  
<https://raysinut.signin.aws.amazon.com/console>

Customize | Copy Link

**IAM Resources**

Users: 1	Roles: 0
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

**Security Status**

5 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input checked="" type="checkbox"/> Activate MFA on your root account	▼
<input checked="" type="checkbox"/> Create individual IAM users	▼
<input checked="" type="checkbox"/> Use groups to assign permissions	▼
<input checked="" type="checkbox"/> Apply an IAM password policy	▼

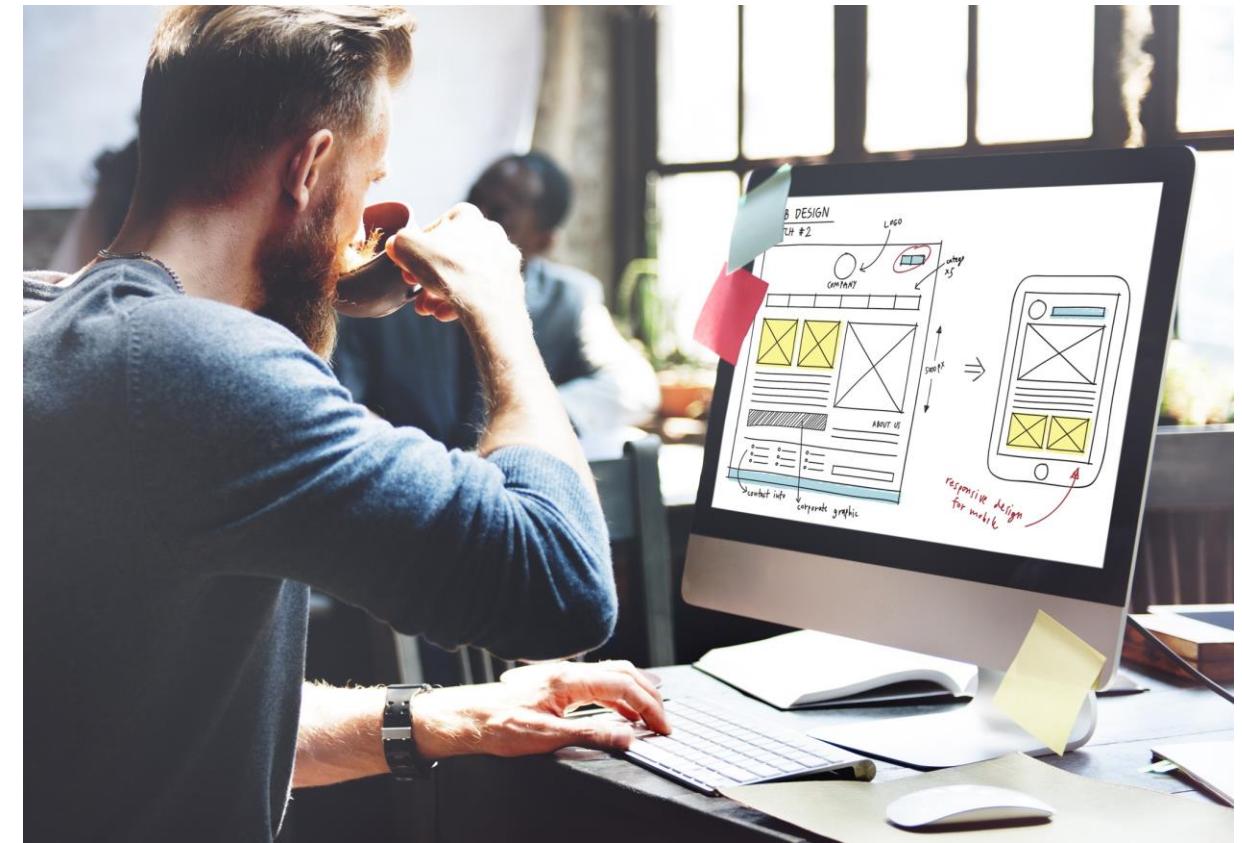
# Principais lições da Seção 3



Práticas recomendadas para proteger uma conta da AWS:

- **Proteja** os logins com Multi-Factor Authentication (MFA).
- **Exclua chaves de acesso** do usuário raiz da conta.
- **Crie usuários do IAM** individuais e conceda permissões de acordo com o princípio do privilégio mínimo.
- **Use grupos** para atribuir permissões a usuários do IAM.
- **Configure** uma **política de senha forte**.
- **Delegue** usando **funções** em vez de compartilhar credenciais.
- **Monitore** a atividade da conta usando o AWS CloudTrail.

# Laboratório 1: Introdução ao IAM



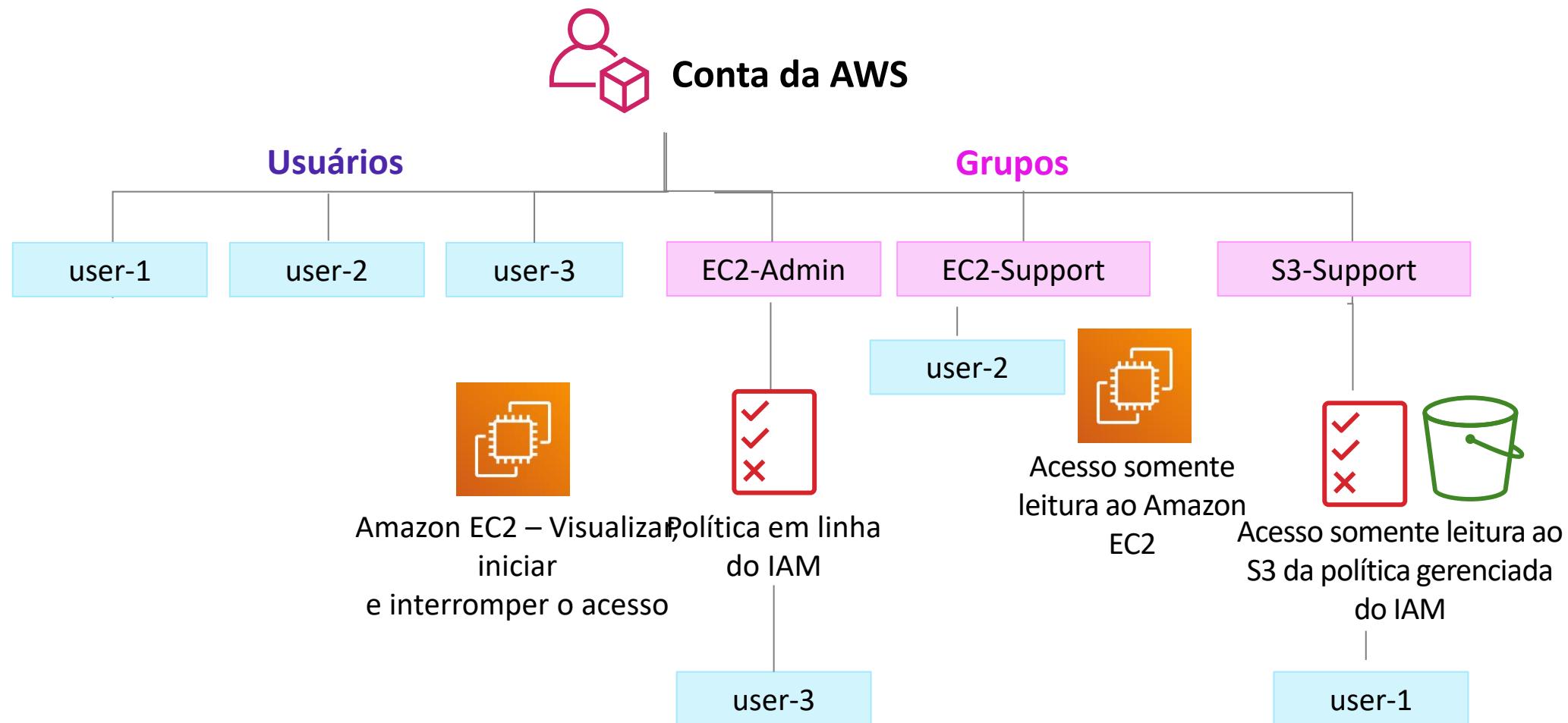
# Laboratório 1: Tarefas

- Tarefa 1: explorar usuários e grupos.
- Tarefa 2: adicionar usuários aos grupos.
- Tarefa 3: fazer login e testar usuários.



AWS Identity and  
Access Management (IAM)

# Laboratório 1: Produto final





Aproximadamente  
40 minutos



## Comece o Laboratório 1: introdução ao AWS IAM

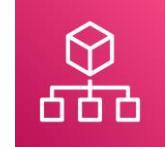
# Resumo do laboratório: principais lições



Módulo 4: Segurança na Nuvem AWS

## Seção 4: Proteção de contas

- O **AWS Organizations** permite consolidar várias contas da AWS para que você as gerencie de maneira centralizada.



AWS Organizations

- Recursos de segurança do AWS Organizations:

- **Agrupe contas da AWS em unidades organizacionais** (OUs) e anexe políticas de acesso diferentes a cada OU.
- **Integração e suporte para o IAM**
  - As permissões para um usuário são a interseção do que é permitido pelo AWS Organizations e o que é concedido pelo IAM nessa conta.
- **Use políticas de controle de serviço** para estabelecer controle sobre os serviços da AWS e as ações de API que cada conta da AWS pode acessar

# AWS Organizations: políticas de controle de serviço



- As **políticas de controle de serviço (SCPs)** oferecem controle centralizado sobre contas.
  - Limite as permissões disponíveis em uma conta que faça parte de uma organização.
- Garante que as contas estejam em conformidade com as diretrizes de controle de acesso.
- As SCPs são *semelhantes* às políticas de permissões do IAM –
  - Elas usam uma sintaxe semelhante.
  - No entanto, uma SCP nunca concede permissões.
  - Em vez disso, as SCPs **especificam as permissões máximas** para uma organização.

- Recursos do **AWS Key Management Service (AWS KMS)**:
  - Permite **criar e gerenciar chaves de criptografia**
  - Permite controlar o uso da criptografia nos serviços da AWS e nos aplicativos.
  - Integra-se ao AWS CloudTrail para registrar todo o uso de chaves.
  - Usa módulos de segurança de hardware (HSMs) validados pelo Federal Information Processing Standards (FIPS) 140-2 para proteger chaves



AWS Key Management  
Service (AWS KMS)

- Recursos do **Amazon Cognito**:

- Adiciona inscrição, login e controle de acesso de usuários a aplicativos Web e móveis.
- Ajusta a escala até milhões de usuários.
- Oferece suporte a login com provedores de identidade social, como Facebook, Google e Amazon, e provedores de identidade corporativa, como o Microsoft Active Directory por meio do Security Assertion Markup Language (SAML) 2.0.



Amazon Cognito

- Recursos do **AWS Shield**:
  - É um serviço gerenciado de proteção contra negação de serviço distribuída (DDoS)
  - Protege aplicativos executados na AWS
  - Fornece detecção sempre ativada e mitigações automáticas em linha
  - *AWS Shield Standard* habilitado sem custo adicional. O *AWS Shield Advanced* é um serviço pago opcional.
- Use-o para **minimizar o tempo de inatividade e a latência do aplicativo.**



AWS Shield

Módulo 4: Segurança na Nuvem AWS

# Seção 5: Proteção de dados na AWS

# Criptografia de dados *em repouso*



- A **criptografia** codifica dados com uma **chave secreta**, o que os torna ilegíveis

- Somente quem tem a chave secreta pode decodificar os dados
  - O **AWS KMS** pode gerenciar suas chaves secretas



- A AWS oferece suporte à criptografia de **dados em repouso**

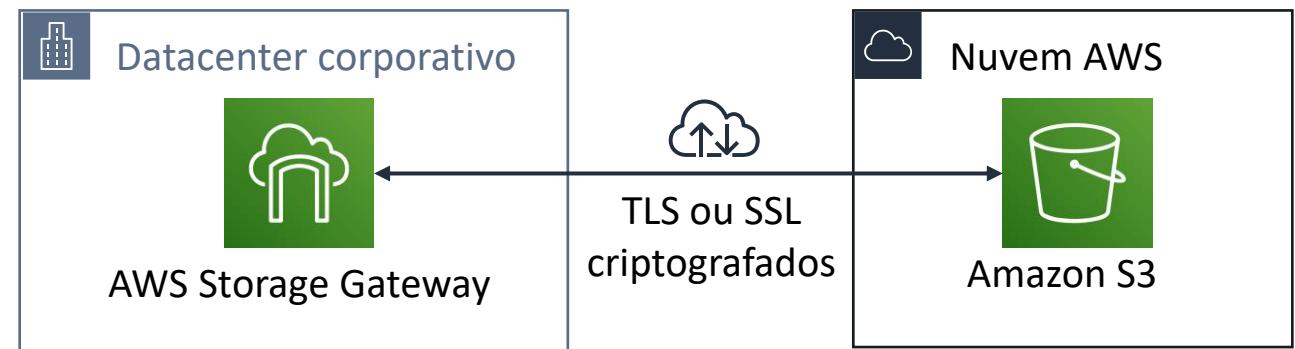
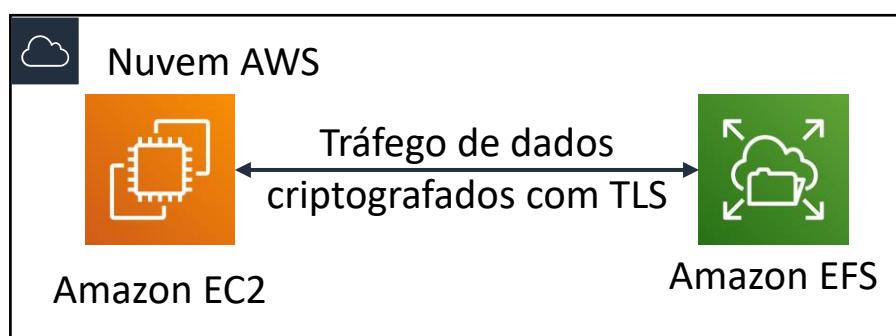
- Dados em repouso = dados armazenados fisicamente (em disco ou fita)
  - Você pode criptografar dados armazenados em qualquer serviço compatível com o AWS KMS, incluindo:
    - Amazon S3
    - Amazon EBS
    - Amazon Elastic File System (Amazon EFS)
    - Bancos de dados gerenciados do Amazon RDS



# Criptografia de dados *em trânsito*



- Criptografia de **dados em trânsito** (dados em movimentação por uma rede)
  - **Transport Layer Security (TLS)**, anteriormente SSL, é um protocolo de padrão aberto
  - **AWS Certificate Manager** oferece uma maneira de gerenciar, implantar e renovar certificados TLS ou SSL
- O HTTP seguro (HTTPS) cria um túnel seguro
  - Ele usa TLS ou SSL para a troca bidirecional de dados
- **Os serviços da AWS oferecem suporte à criptografia de dados em trânsito.**
  - Dois exemplos:



- Os buckets e objetos do S3 recém-criados são **privados e protegidos** por padrão.
- Quando os casos de uso exigem o compartilhamento de objetos de dados no Amazon S3 –
  - É essencial gerenciar e controlar o acesso aos dados.
  - Siga as **permissões que respeitam o princípio do privilégio mínimo** e considere o uso da criptografia do Amazon S3.
- Ferramentas e opções para controlar o acesso aos dados do S3 incluem –
  - Recurso Amazon S3 Block Public Access: simples de usar.
  - Políticas do IAM: uma boa opção quando o usuário pode autenticar usando o IAM.
  - Políticas de buckets
  - Listas de controle de acesso (ACLs): um mecanismo de controle de acesso herdado.
  - Verificação de permissão de bucket do AWS Trusted Advisor: um recurso gratuito.

Módulo 4: Segurança na Nuvem AWS

# Seção 6: Trabalhar para garantir a conformidade

# Programas de conformidade da AWS



- Os clientes estão sujeitos a muitos regulamentos e requisitos diferentes de segurança e conformidade.
- A AWS contrata órgãos de certificação e auditores independentes para fornecer aos clientes informações detalhadas sobre as políticas, os processos e os controles estabelecidos e operados pela AWS.
- Os programas de conformidade podem ser categorizados amplamente –
  - **Certificações e declarações**
    - Avaliado por um auditor externo independente
    - Exemplos: ISO 27001, 27017, 27018 e ISO/IEC 9001
  - **Leis, regulamentos e privacidade**
    - A AWS fornece recursos de segurança e contratos legais para apoiar a conformidade
    - Exemplos: Regulamento geral de proteção de dados (GDPR), da UE, HIPAA
  - **Alinhamentos e estruturas**
    - Requisitos de segurança ou conformidade específicos do setor ou da função
    - Exemplos: Center for Internet Security (CIS), certificado Privacy Shield entre UE e EUA





AWS Config

## Exemplo de exibição do painel do AWS Config

The screenshot shows the AWS Config Dashboard with the following data:

Resource Type	Count
Total resource count	48
Top 10 resource types	Total
EC2 SecurityGroup	8
Lambda Function	7
S3 Bucket	6
EC2 Subnet	6
CloudWatch Alarm	3
EC2 InternetGateway	2
EC2 Instance	2
EC2 VPC	2
EC2 NetworkInterface	2
EC2 RouteTable	2

**Config rule compliance:** 1 Noncompliant rule(s)

**Resource compliance:** 35 Noncompliant resource(s)

**Noncompliant rules:**

Rule name	Compliance
required-tags	25+ noncompliant resource(s)

- Avalie e audite as configurações dos recursos da AWS.
- Use para monitoramento contínuo de configurações.
- Avalie automaticamente as configurações *registradas* em comparação com as configurações *desejadas*.
- Analise as alterações de configuração.
- Visualize os históricos de configuração detalhados.
- Simplifique a auditoria de conformidade e a análise de segurança.



AWS Artifact

- É um recurso para informações relacionadas à conformidade
- Forneça acesso a relatórios de segurança e conformidade e selecione contratos on-line
- É possível acessar exemplos de downloads:
  - Certificações ISO da AWS
  - Relatórios do Payment Card Industry (PCI) e do Service Organization Control (SOC)
- Acesse o AWS Artifact diretamente do Console de Gerenciamento da AWS
  - Em **Security, Identify & Compliance** (Segurança, Identificação e Conformidade), clique em **Artifact** (Artefato).

# Principais lições da Seção 6



- Os **programas de conformidade de segurança da AWS** fornecem informações sobre as políticas, os processos e os controles estabelecidos e operados pela AWS.
- O **AWS Config** é usado para avaliar e auditar as configurações dos recursos da AWS.
- O **AWS Artifact** fornece acesso a relatórios de segurança e conformidade.

Módulo 4: Segurança na Nuvem AWS

## Seção 7: Serviços e recursos de segurança adicionais



AWS Service  
Catalog

- **Crie e gerencie catálogos de serviços de TI aprovados pela sua organização**
  - Ajuda os funcionários a encontrar e implantar serviços de TI *aprovados*
  - Um serviço de TI pode incluir um ou mais recursos da AWS
  - Exemplo:
    - Instâncias do EC2, volumes de armazenamento, bancos de dados e componentes de rede
- Controle o uso do serviço da AWS especificando restrições –
  - Exemplos de restrições:
    - A região da AWS em que um produto pode ser lançado
    - Intervalos de endereços IP permitidos
- Gerencie o ciclo de vida de serviços de TI centralizada
- Ajude a cumprir requisitos de conformidade

# Serviços de segurança adicionais selecionados



Amazon  
Macie

**Proteja proativamente informações de identificação pessoal (PII)** e saiba quando elas se movimentam.



Amazon  
Inspector

Defina os padrões e as melhores práticas para seus aplicativos e **valide a adesão** a esses **padrões**.



Amazon  
GuardDuty

**Detecção de ameaças** inteligente e monitoramento contínuo para proteger contas e cargas de trabalho da AWS.

Módulo 4: Segurança na Nuvem AWS

# Conclusão do módulo

Resumindo, neste módulo você aprendeu a:

- Reconhecer o modelo de responsabilidade compartilhada
- Identificar a responsabilidade do cliente e a da AWS
- Reconhecer usuários, grupos e funções do IAM
- Descrever diferentes tipos de credenciais de segurança no IAM
- Identificar as etapas para a proteção de novas contas da AWS
- Explorar usuários e grupos do IAM
- Reconhecer como proteger dados da AWS
- Reconhecer programas de conformidade da AWS

# Conclua o teste de conhecimento



# Exemplo de pergunta do exame



Qual das opções a seguir é responsabilidade da AWS segundo o modelo de responsabilidade compartilhada da AWS?

- A. Configuração de aplicativos de terceiros
- B. Manutenção de hardware físico
- C. Proteção de acesso e dados de aplicativos
- D. Gerenciamento de imagens de máquina da Amazon (AMIs) personalizadas

# Recursos adicionais



- Página inicial [de segurança da Nuvem AWS](#)
- [Recursos de segurança da AWS](#)
- [Blog de segurança da AWS](#)
- [Boletins de segurança](#)
- [Teste de vulnerabilidade e penetração](#)
- AWS Well-Architected Framework – [Pilar da segurança](#)
- Documentação da AWS – [Práticas recomendadas do IAM](#)

# Obrigado