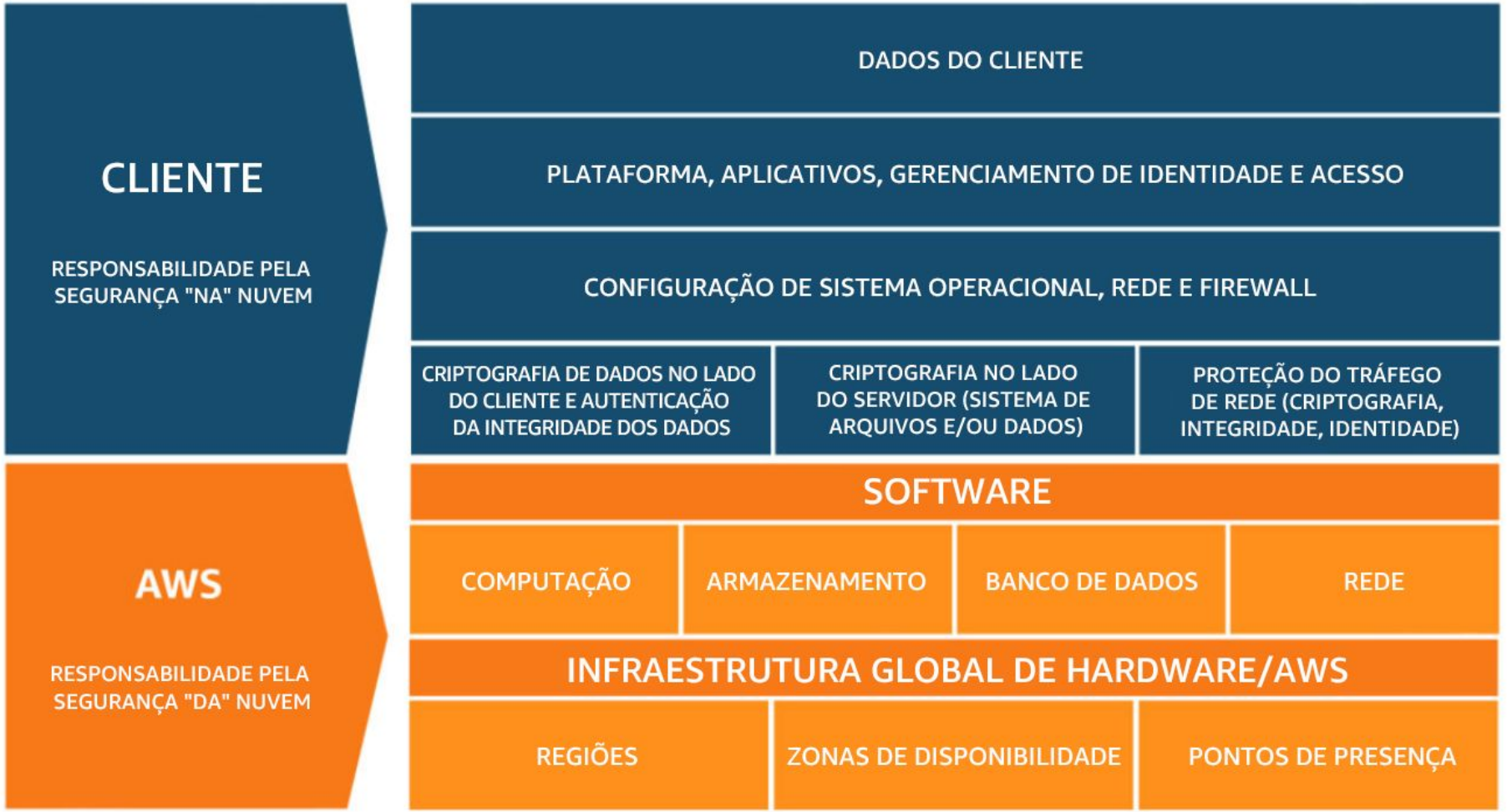
AWS Academy Cloud Foundations (Fundamentos de nuvem da AWS Academy)

Módulo 4: Segurança na Nuvem AWS

Módulo 4: Segurança na Nuvem AWS

Seção 1: Modelo de responsabilidade compartilhada da AWS

Modelo de responsabilidade compartilhada da AWS

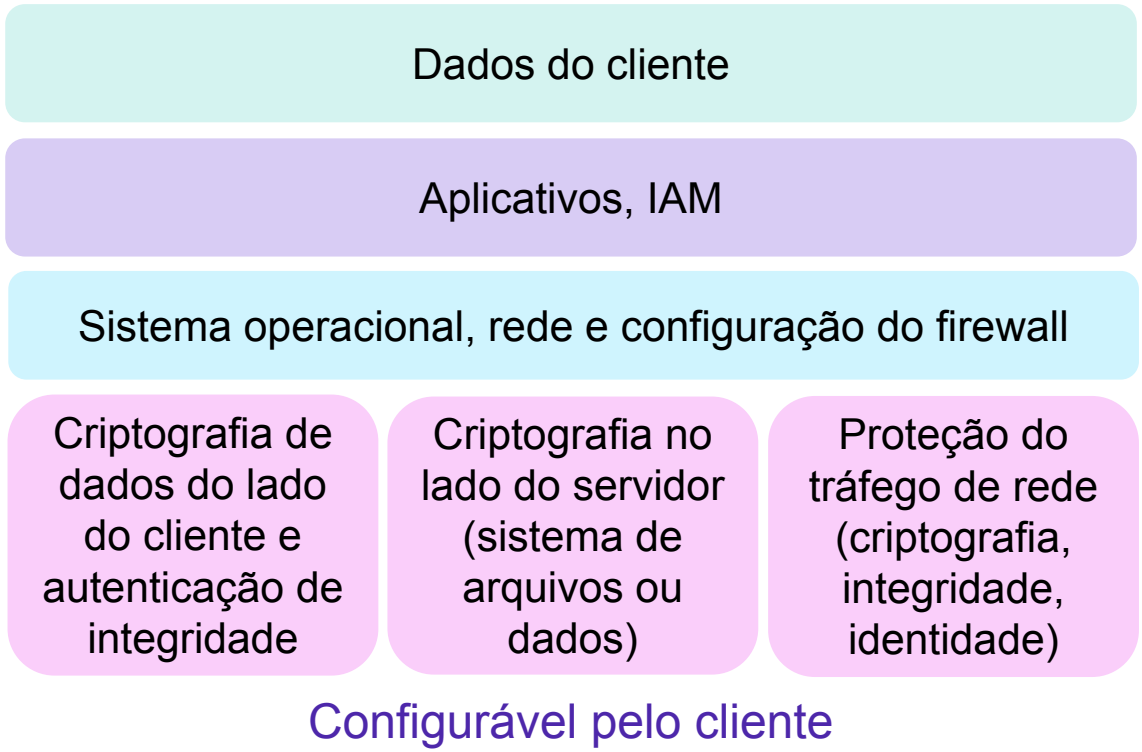


Responsabilidade da AWS: segurança *da* nuvem

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 au
- Infraestrutura de rede
  - Detecção de intrusão
- Infraestrutura de virtualização
  - Isolamento de instância

Responsabilidade do cliente: segurança *na* nuvem

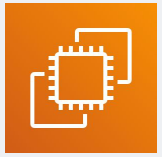


Responsabilidades do cliente:

- 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)

Serviços de exemplo gerenciados pela AWS

AWS Lambda

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

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

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)

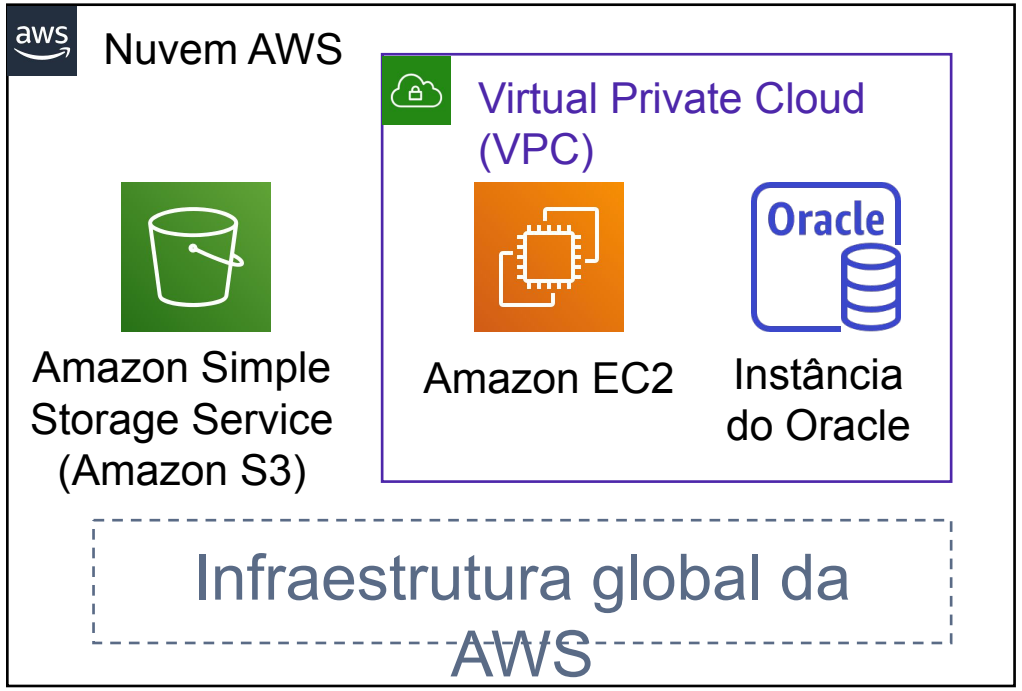
- O software é hospedado de maneira centralizada
- Licenciado em um modelo de assinatura ou pagamento conforme o uso.
- Os serviços normalmente são acessados por meio de um navegador da Web, um aplicativo móvel ou uma interface de programação de aplicativos (API)
- Os clientes não precisam gerenciar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

Atividade: modelo de responsabilidade compartilhada da AWS

Foto de Pixabay da Pexels.

Atividade: cenário 1 de 2

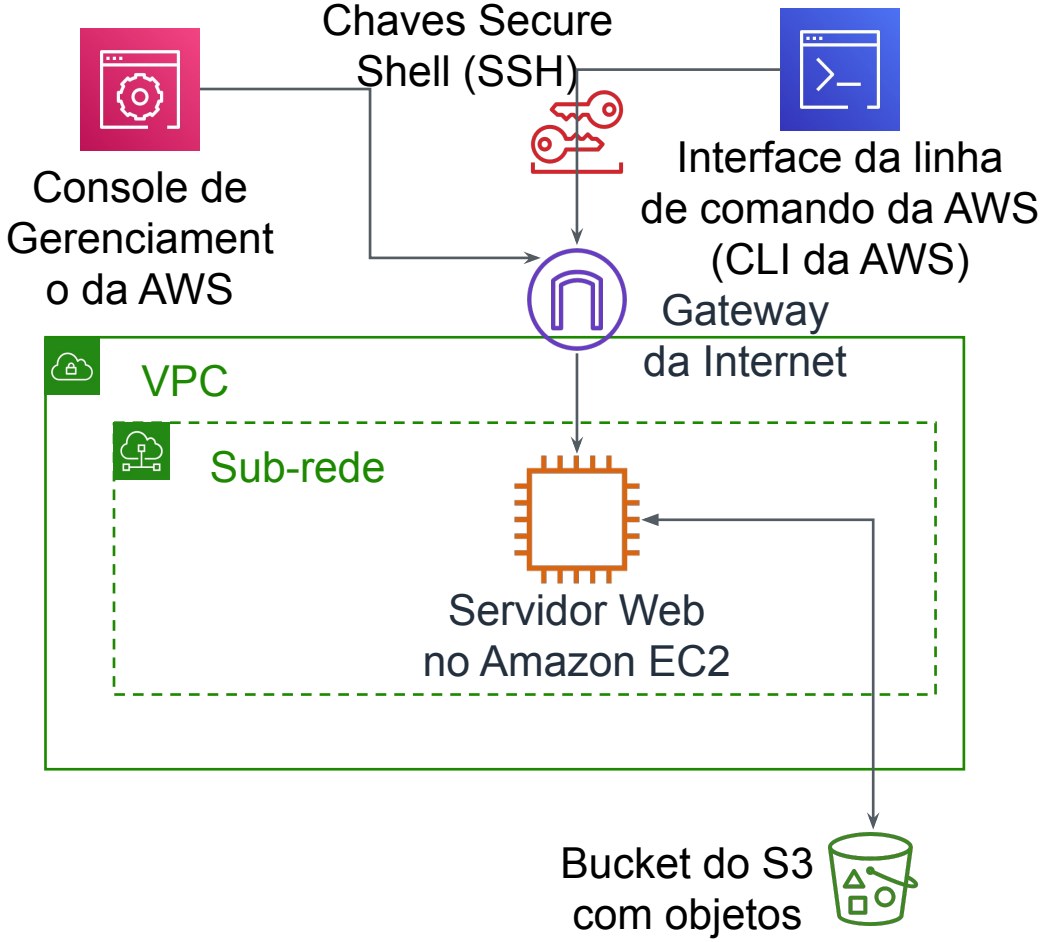
Considere esta implantação. Quem é responsável, a AWS ou o cliente?



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

Considere 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. Impor a Multi-Factor Authentication para todos os logins de usuário?
   - **RESPOSTA:** o cliente

Principais lições da Seção 1

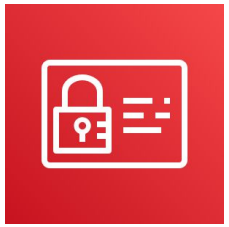
- A AWS e o cliente compartilham responsabilidades de segurança:
  - A AWS é responsável pela segurança da nuvem
  - O cliente é responsável pela segurança na nuvem
- **A AWS é responsável por proteger a infraestrutura** que executa os serviços de nuvem AWS, incluindo hardware, software, redes e instalações
- 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)

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



AWS Identity and Access Management (IAM)

- *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

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*

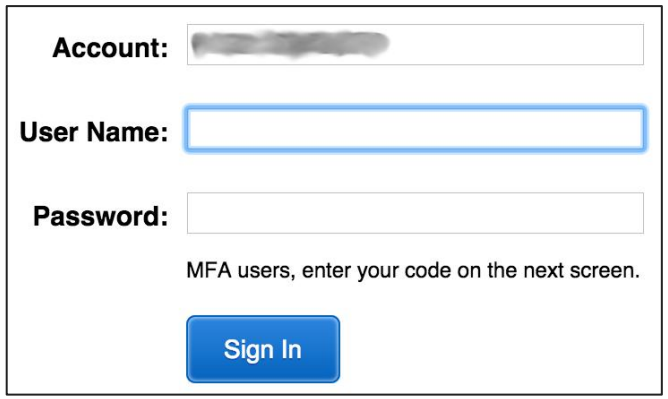
- Autentique usando:
  - ID *ou* alias da conta com 12 dígitos
  - Nome de usuário do IAM
  - Senha do IAM
- Se ativada, a **Multi-Factor Authentication (MFA)** solicita um código de autenticação.

Console de Gerenciamento da AWS

MFA do IAM

- A MFA oferece maior segurança.

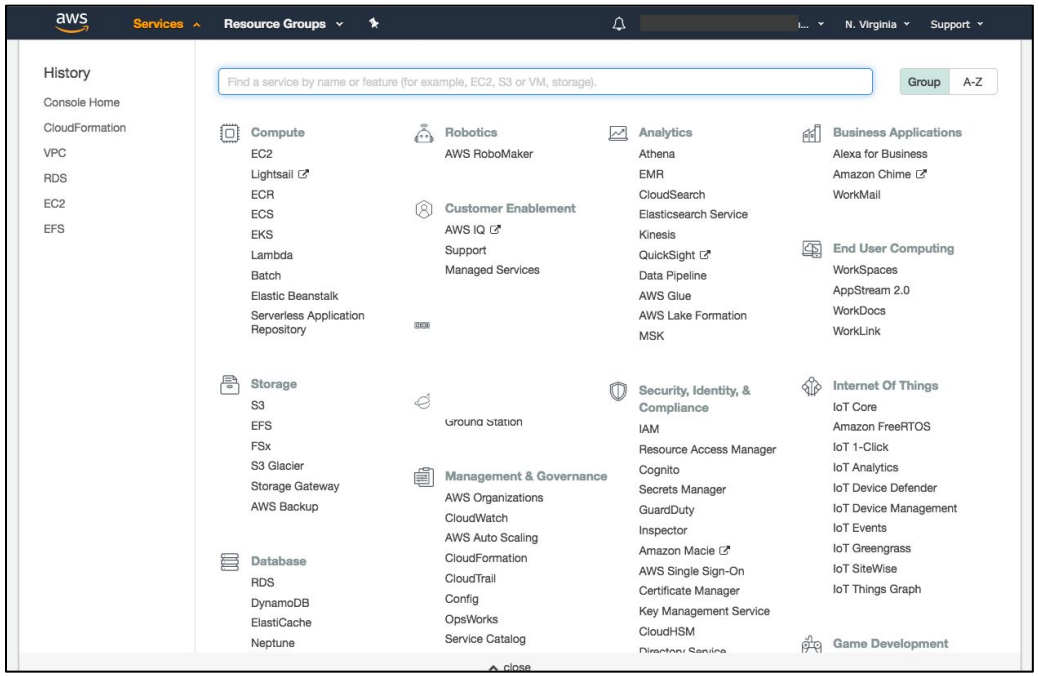
- Além **do nome de usuário** e da **senha**, a MFA requer um código de autenticação exclusivo para acessar os serviços da AWS.



Nome de usuário e senha

MFA

Token de MFA



Console de Gerenciamento da AWS

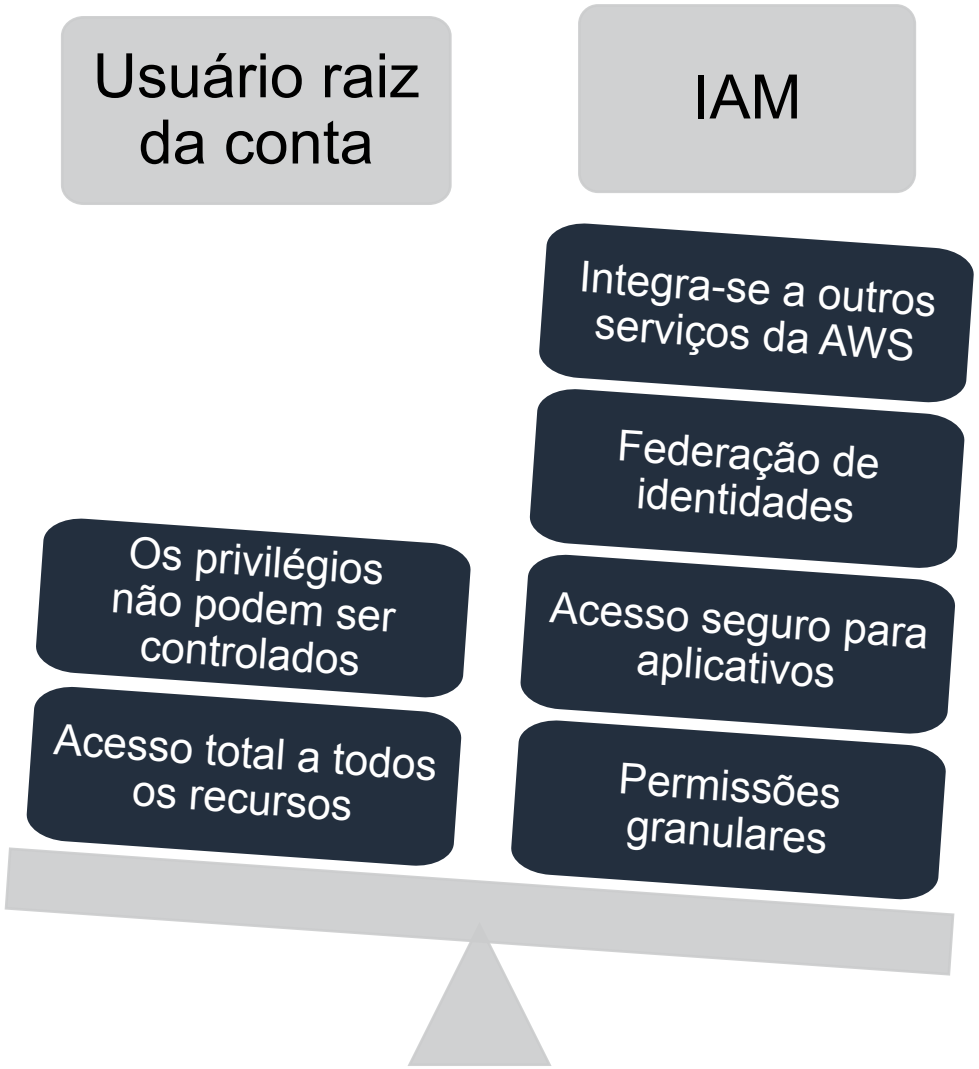
Principais lições da Seção 2

- 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.

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: MFA

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).

Proteção de novas contas da AWS: relatórios de faturamento

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.

Principais lições da Seção 3

Práticas recomendadas para proteger uma conta da AWS:

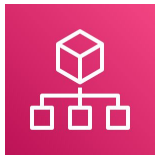
- **Proteja** os logins com Multi-Factor Authentication (MFA).
- **Exclua** chaves de acesso do usuário raiz da conta.
- **Crie** usuários do IAM individuais e conceda permissões de acordo com o princípio do privilégio mínimo.
- **Use grupos** para atribuir permissões a usuários do IAM.
- **Configure**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

Módulo 4: Segurança na Nuvem AWS

Seção 4: Proteção de contas

AWS Organizations

- 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 Key Management Service (AWS KMS)

- 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)

Amazon Cognito

- 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

AWS Shield

- 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 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

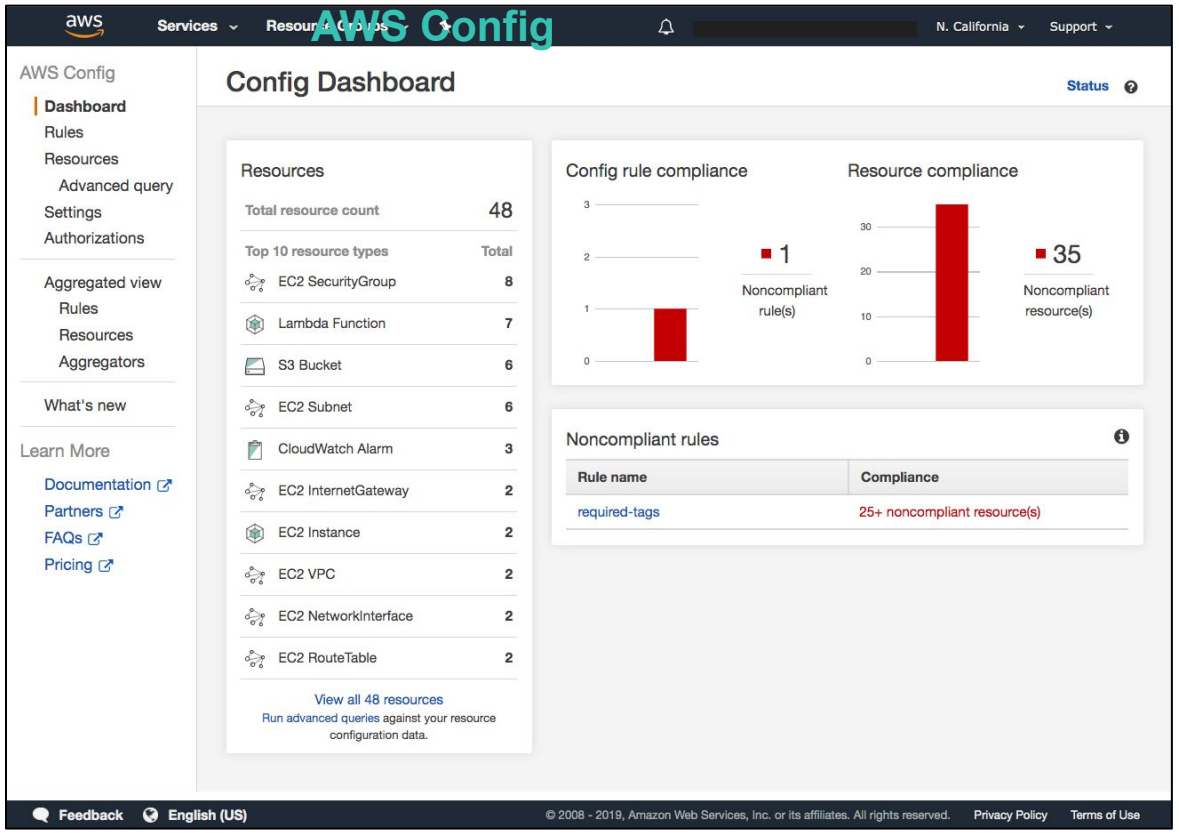
  - **Leis, regulamentos e privacidade**
    - A AWS fornece recursos de segurança e contratos legais para apoiar a conformidade
    - Exemplos: Regulamento geral de proteção de dados (GDPR), da UE, HIPAA

  - **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

AWS Config

Exemplo de exibição do painel do AWS Config



- **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

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.

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