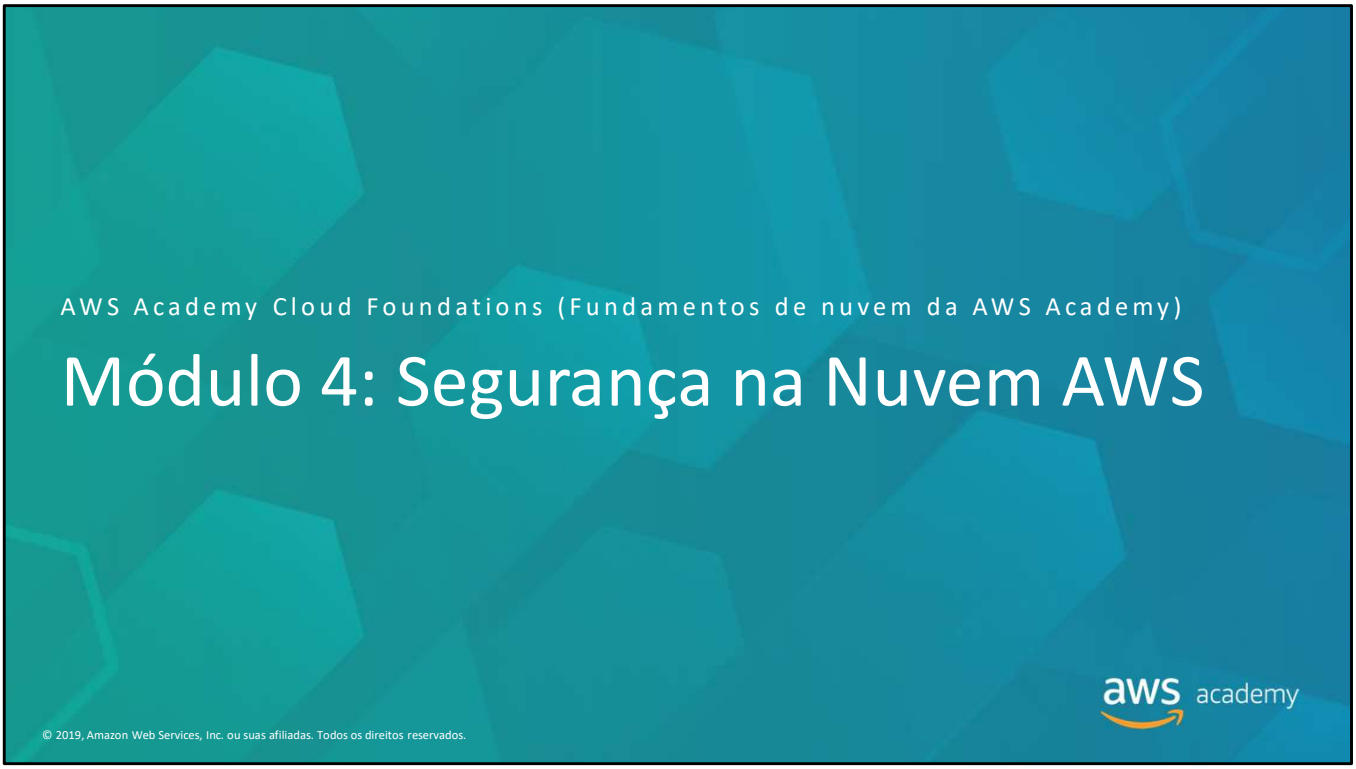


Bem-vindo ao Módulo 4: Segurança na Nuvem AWS.

A segurança é a maior prioridade na Amazon Web Services (AWS). A AWS oferece um ambiente de computação em nuvem escalável projetado para oferecer alta disponibilidade e confiabilidade, além de fornecer as ferramentas que permitem executar uma grande variedade de aplicativos. Ajudar a proteger a confidencialidade, a integridade e a disponibilidade de seus sistemas e dados é essencial para a AWS, assim como manter a confiança e a convicção do cliente. Este módulo fornece uma introdução à abordagem da AWS à segurança, que inclui os controles no ambiente da AWS e alguns dos produtos e recursos da AWS que os clientes podem usar para cumprir os objetivos de segurança.

Visão geral do módulo

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

Este módulo abordará os seguintes 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
- Serviços e recursos de segurança adicionais

A Seção 1 inclui uma **atividade** com instrutor no modelo de responsabilidade compartilhada da AWS.

A Seção 2 inclui uma demonstração do **IAM gravada**, e o final dessa mesma seção inclui um **laboratório prático** para você praticar como configurar o IAM usando o Console de Gerenciamento da AWS.

Por fim, você deverá concluir um **teste de conhecimento** para testar sua compreensão dos principais conceitos abordados neste módulo.

Objetivos do módulo

aws academy

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

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

aws academy

Apresentação da Seção 1: Modelo de responsabilidade compartilhada da AWS.

Modelo de responsabilidade compartilhada da AWS

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Esse modelo de responsabilidade compartilhada foi projetado para ajudar a reduzir a carga operacional do cliente. Ao mesmo tempo, para oferecer a flexibilidade e o controle do cliente que permitem a implantação de soluções de clientes na AWS, o cliente permanece responsável por alguns aspectos da segurança geral. A diferenciação de quem é responsável pelo quê normalmente se dá pelas expressões *segurança "da" nuvem* e *segurança "na" nuvem*.

A **AWS** opera, gerencia e controla os componentes desde a camada de virtualização de software até a segurança física das instalações em que os serviços da AWS operam. **A AWS é responsável** pela proteção da infraestrutura que executa todos os serviços oferecidos na Nuvem AWS. Essa infraestrutura é composta por hardware, software, redes e instalações que executam os Serviços de nuvem AWS.

O cliente é responsável pela criptografia de dados em repouso e em trânsito. O cliente também deve garantir que a rede esteja configurada para segurança e que as credenciais e os logins de segurança sejam gerenciados de maneira segura. Além disso, o cliente é responsável pela configuração de grupos de segurança e pela configuração do sistema operacional que é executado nas instâncias de computação que ele executa (incluindo atualizações e patches de segurança).

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

A AWS é responsável pela segurança ***da*** nuvem. Mas o que isso significa?

Sob o modelo de responsabilidade compartilhada da AWS, a AWS opera, gerencia e controla os componentes do sistema operacional host bare metal e da camada de virtualização do hipervisor até a segurança física das instalações em que os serviços operam. Isso significa que a AWS é responsável pela proteção da infraestrutura global que executa todos os serviços oferecidos na Nuvem AWS. A infraestrutura global inclui zonas de disponibilidade, pontos de presença e regiões da AWS.

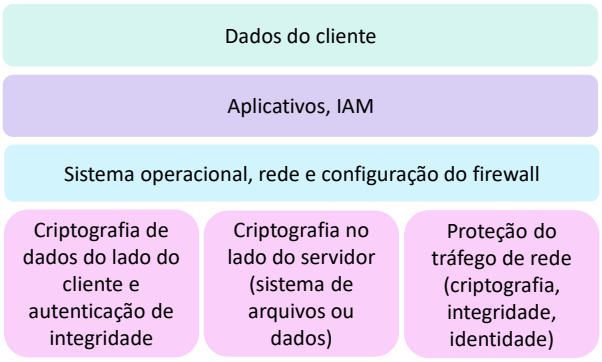
A AWS é responsável pela infraestrutura física que hospeda seus recursos, incluindo:

- **Segurança física de datacenters** com acesso controlado e baseado em necessidades; localizados em instalações não identificadas, com guardas de segurança 24 horas por dia, 7 dias por semana; autenticação de dois fatores; revisão e registro em log de acesso; vigilância por vídeo; e desmagnetização e destruição de discos.
- **Infraestrutura de hardware**, como servidores, dispositivos de armazenamento e outros dispositivos dos quais a AWS depende.
- **Infraestrutura de software**, que hospeda sistemas operacionais, aplicativos de serviço e software de virtualização.
- **Infraestrutura de rede**, como roteadores, switches, load balancers, firewalls e cabeamento. A AWS também monitora continuamente a rede em limites externos,

protege pontos de acesso e oferece infraestrutura redundante com detecção de intrusão.

A proteção dessa infraestrutura é a maior prioridade da AWS. Embora você não possa visitar datacenters ou escritórios da AWS para ver essa proteção em primeira mão, a Amazon fornece vários relatórios de auditores terceirizados que verificaram nossa conformidade com diversos padrões e regulamentos de segurança de computadores.

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

Embora a infraestrutura de nuvem seja protegida e mantida pela AWS, os clientes são responsáveis pela segurança de tudo o que colocam ***na*** nuvem.

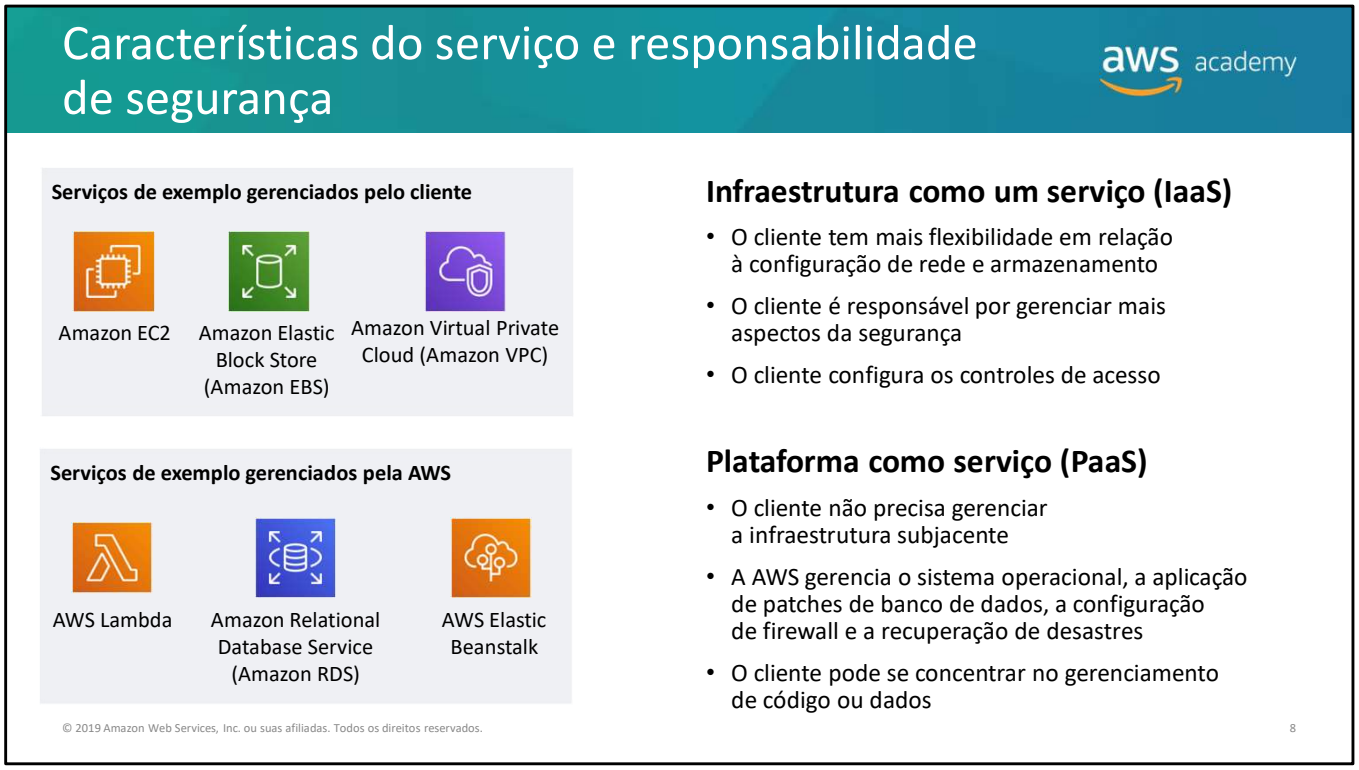
O **cliente é responsável** pelo que é implementado com o uso dos serviços da AWS e pelos aplicativos conectados à AWS. As etapas de segurança que você deve seguir dependem dos serviços que você usa e da complexidade do seu sistema.

As responsabilidades do cliente incluem selecionar e proteger qualquer sistema operacional de instância, proteger os aplicativos executados em recursos da AWS, configurações de grupos de segurança, configurações de firewall, configurações de rede e gerenciamento seguro de contas.

Quando os clientes usam os serviços da AWS, eles mantêm controle total sobre o conteúdo. Os clientes são responsáveis por gerenciar requisitos críticos de segurança de conteúdo, incluindo:

- Qual conteúdo eles escolhem armazenar na AWS
- Quais serviços da AWS são usados com o conteúdo
- Em qual país esse conteúdo é armazenado
- O formato e a estrutura desse conteúdo e se ele é mascarado, anonimizado ou criptografado
- Quem tem acesso a esse conteúdo e como esses direitos de acesso são concedidos, gerenciados e revogados

Os clientes mantêm o controle da segurança que escolhem implementar para proteger seus próprios dados, ambiente, aplicativos, configurações do IAM e sistemas operacionais.



Infraestrutura como serviço (IaaS) refere-se a serviços que fornecem componentes básicos da TI, normalmente incluindo acesso para configuração de redes, computadores (virtuais ou em hardware dedicado) e espaço para o armazenamento de dados. Os serviços de nuvem que podem ser caracterizados como IaaS **fornecem ao cliente o mais alto nível de flexibilidade e controle de gerenciamento** sobre recursos de TI. Os serviços de IaaS são mais semelhantes aos recursos de computação locais existentes com os quais muitos departamentos de TI estão familiarizados atualmente.

Os serviços da AWS, como o **Amazon EC2**, podem ser categorizados como **IaaS** e, portanto, **exigem que o cliente execute todas as tarefas de configuração e gerenciamento de segurança necessárias**. Os clientes que implantam instâncias do EC2 são responsáveis pela gestão do sistema operacional convidado (incluindo atualizações e patches de segurança), qualquer software de aplicativo instalado nas instâncias e pela configuração dos grupos de segurança que foram fornecidos pela AWS.

Plataforma como serviço (PaaS) refere-se a serviços que eliminam a necessidade de o cliente gerenciar a infraestrutura subjacente (hardware, sistemas operacionais etc.). Os serviços PaaS permitem que o cliente se concentre totalmente na implantação e no gerenciamento de aplicativos. Os clientes não precisam se preocupar com a aquisição de recursos, o planejamento de capacidade, a manutenção de software ou a aplicação de patches.

Serviços da AWS, como o **AWS Lambda** e o **Amazon RDS,** podem ser categorizados

como **PaaS**, pois a **AWS opera a camada de infraestrutura, o sistema operacional e as plataformas**. Os clientes só precisam acessar os endpoints para armazenar e recuperar dados. Com os serviços PaaS, os clientes são responsáveis por gerenciar os dados, classificar os ativos e aplicar as permissões apropriadas. No entanto, esses serviços atuam mais como serviços gerenciados, com a AWS gerenciando uma parte maior dos requisitos de segurança. No caso desses serviços, a AWS se encarrega das tarefas básicas de segurança, como aplicação de patches em sistemas operacionais e bancos de dados, configuração de firewall e recuperação de desastres.

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

Software como serviço (SaaS) refere-se a serviços que fornecem software hospedado de maneira centralizada que geralmente é acessível por meio de um navegador da Web, aplicativo móvel ou interface de programação de aplicativos (API). O modelo de licenciamento para ofertas de SaaS normalmente é de assinatura ou pagamento conforme o uso. Com as ofertas de SaaS, os clientes não precisam gerenciar a infraestrutura que oferece suporte ao serviço. Alguns serviços da AWS, como **AWS Trusted Advisor, AWS Shield** e **Amazon Chime**, podem ser categorizados como ofertas de SaaS, considerando as características que têm.

O **AWS Trusted Advisor** é uma ferramenta on-line que analisa seu ambiente da AWS e fornece orientações e recomendações em tempo real para ajudar você a provisionar seus recursos seguindo as práticas recomendadas da AWS. O serviço Trusted Advisor é oferecido como parte do seu plano do AWS Support. Alguns dos recursos do Trusted Advisor são gratuitos para todas as contas, mas os clientes do Business Support e do Enterprise Support têm acesso ao conjunto completo de verificações e recomendações do Trusted Advisor.

O **AWS Shield** é um serviço gerenciado de proteção contra a negação de serviço distribuída (DDoS) que protege aplicativos executados na AWS. Ele fornece detecção e mitigações embutidas automáticas e sempre ativas que minimizam o tempo de

inatividade e a latência dos aplicativos. Assim, não é necessário interagir com o AWS Support para ter benefícios de proteção contra DDoS. O AWS Shield Advanced está disponível para todos os clientes. No entanto, para entrar em contato com a equipe de resposta a DDoS, os clientes devem ter o Enterprise Support ou o Business Support do AWS Support.

O **Amazon Chime** é um serviço de comunicação que permite encontrar, conversar e realizar chamadas de negócios dentro e fora da sua organização, usando um só aplicativo. É um serviço de comunicações com pagamento conforme o uso sem taxas adiantadas, compromissos ou contratos de longo prazo.

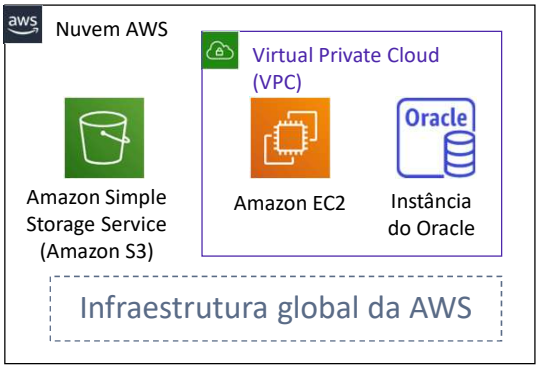
Atividade: modelo de responsabilidade compartilhada da AWS

Foto de Pixabay da Pexels.

Nesta atividade com instrutor, serão apresentados dois cenários. Para cada um deles, serão feitas várias perguntas sobre quem tem a responsabilidade (a AWS ou o cliente) de garantir a segurança do item em questão. O instrutor direcionará a turma em um debate sobre cada pergunta e revelará as respostas corretas, uma de cada vez.

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

Considere o caso em que um cliente usa os serviços e recursos da AWS que são mostrados aqui. Quem é responsável pela manutenção da segurança? A AWS ou o cliente?

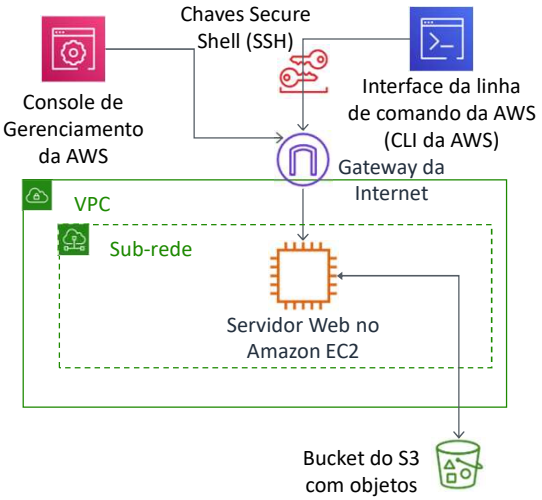
O cliente usa o Amazon Simple Storage Service (Amazon S3) para armazenar dados. O cliente configurou uma virtual private cloud (VPC) com a Amazon Virtual Private Cloud (Amazon VPC). A instância do EC2 e a instância de banco de dados Oracle que ele criou são executadas na VPC.

Neste exemplo, o cliente deve gerenciar o sistema operacional (SO) convidado que é executado na instância do **EC2**. Com o passar do tempo, o sistema operacional convidado precisará ser atualizado e receber a aplicação de patches de segurança. Além disso, qualquer software de aplicativo ou utilitário que o cliente instalou na instância do Amazon EC2 também deve passar por manutenção. O cliente é responsável pela configuração do firewall da AWS (ou grupo de segurança) aplicado à instância do Amazon EC2. O cliente também é responsável pelas configurações da **VPC** que especificam as condições de rede nas quais a instância do Amazon EC2 é executada. Essas tarefas são as mesmas tarefas de segurança que uma equipe de TI executaria, não importa onde seus servidores estivessem localizados.

A instância Oracle neste exemplo fornece um estudo de caso interessante em termos de responsabilidade da AWS ou do cliente. **Se o banco de dados for executado em uma instância do EC2**, será responsabilidade do cliente aplicar atualizações e patches de software da Oracle. No entanto, **se o banco de dados for executado como uma instância do Amazon RDS**, será responsabilidade da AWS aplicar atualizações e patches de software da Oracle. Como o Amazon RDS é uma oferta de banco de dados gerenciada, as tarefas demoradas de administração de banco de dados (que incluem provisionamento, backups, aplicação de patches de software, monitoramento e escalabilidade de hardware) são processadas pela AWS. Para saber mais, consulte Melhores práticas para a execução de bancos de dados Oracle na AWS e veja os detalhes.

Atividade: cenário 2 de 2

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

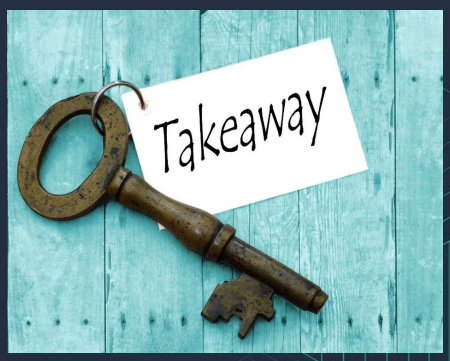


1. Garantir que o Console de Gerenciamento da AWS não seja invadido?
   - **RESPOSTA:** AWS
2. Configurar a sub-rede?
   - **RESPOSTA:** o cliente
3. Configurar a VPC?
   - **RESPOSTA:** o cliente
4. Proteger contra interrupções de rede nas regiões da AWS?
   - **RESPOSTA:** AWS
5. Proteger as chaves 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

Agora, considere esse caso adicional em que um cliente usa os serviços e recursos da AWS que são mostrados aqui. Quem é responsável pela manutenção da segurança? A AWS ou o cliente?

Um cliente usa o Amazon S3 para armazenar dados. Ele configurou uma virtual private cloud (VPC) com a Amazon VPC e está executando um servidor Web em uma instância do EC2 na VPC. O cliente configurou um gateway da Internet como parte da VPC para que o servidor Web possa ser acessado com o uso do Console de Gerenciamento da AWS ou da Interface da Linha de Comando da AWS (CLI da AWS). Quando o cliente usa a CLI da AWS, a conexão requer o uso de chaves Secure Shell (SSH).

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

Algumas das principais lições desta seção do módulo são:

- 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

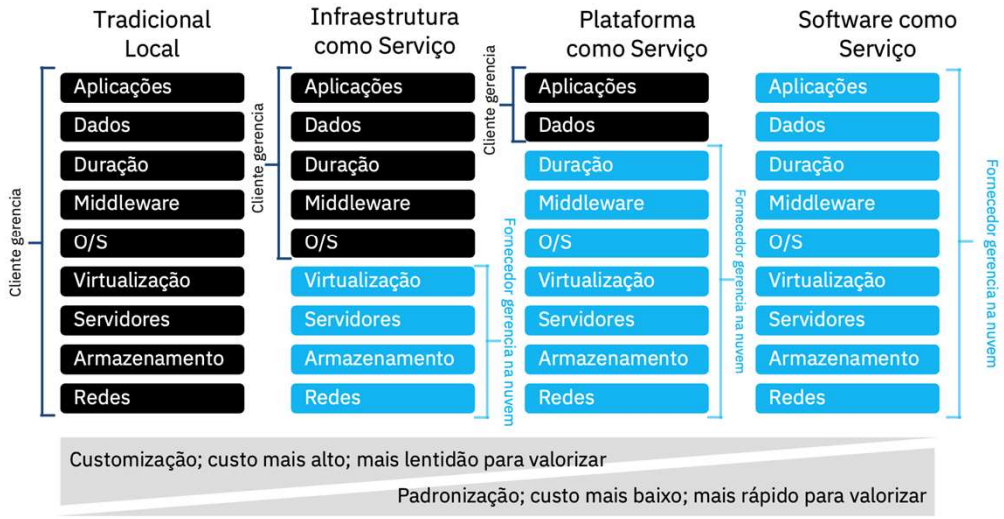
Módulo 4: Segurança na Nuvem AWS

Seção 2: AWS Identity and Access Management (IAM)

aws academy

Apresentação da Seção 2: AWS Identity and Access Management (ou IAM).

Modelos de serviços em nuvem



Customização; custo mais alto; mais lentidão 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[2]

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!

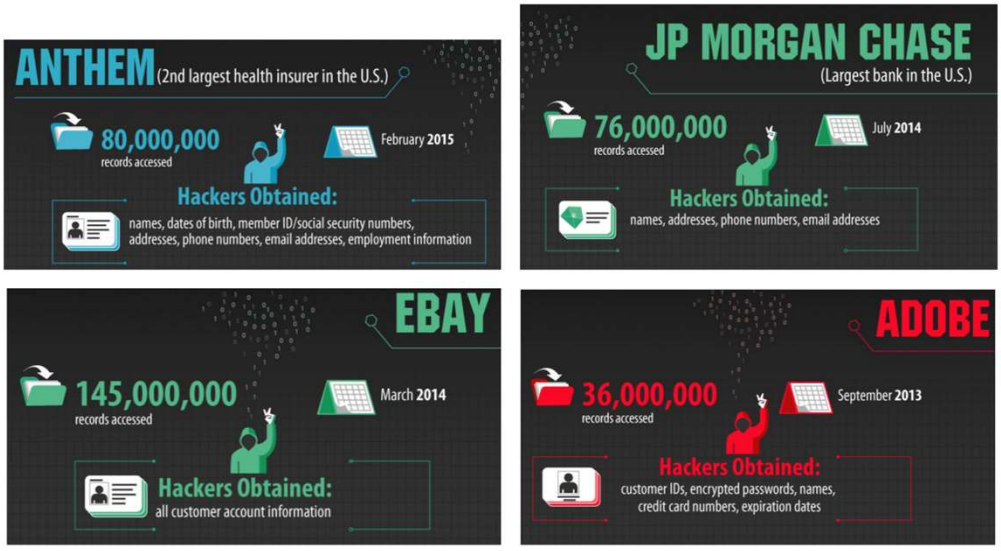
614%

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%

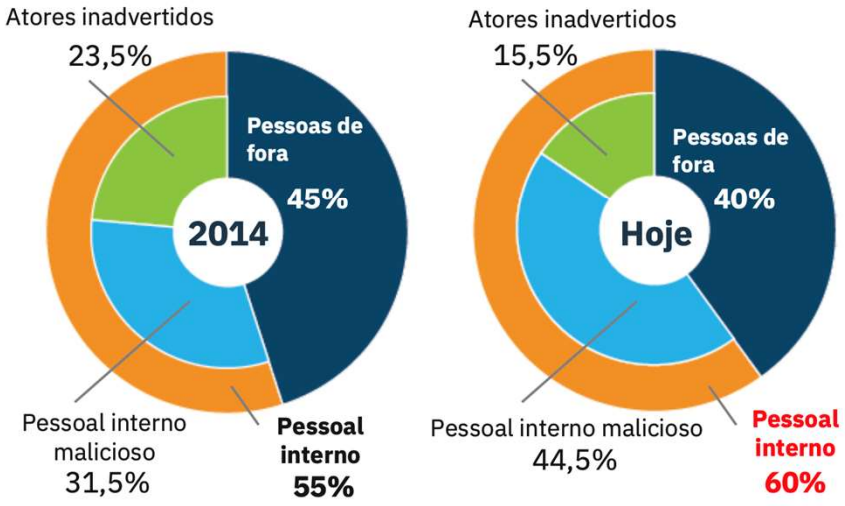
dos executivos senior de TI disseram que planejam armazenar dados em novos ambientes de tecnologia, como a nuvem[1]

Desses, 85% estavam "preocupados" ou "muito preocupados" com a segurança na nuvem[1]

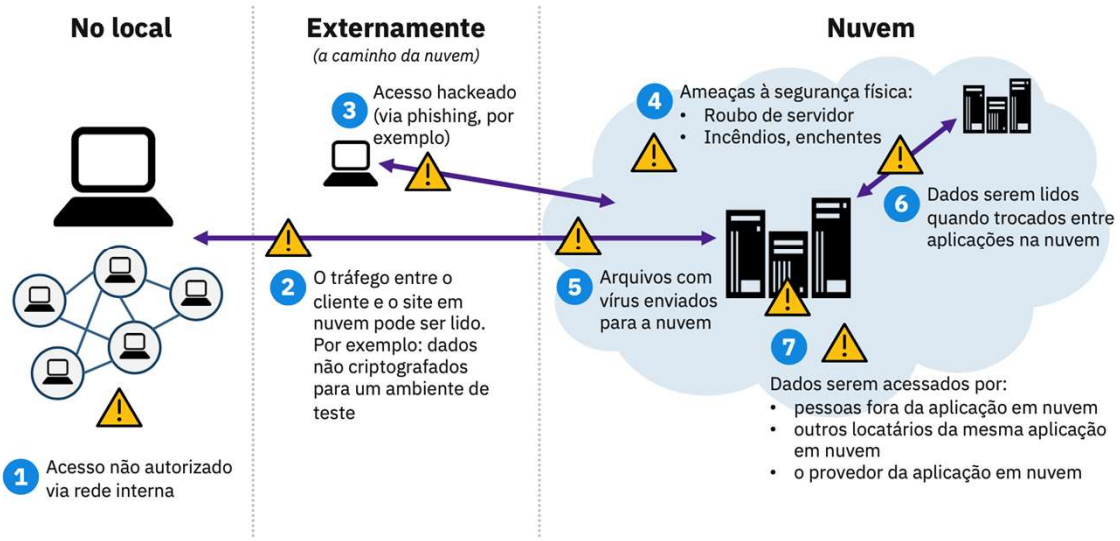
1 *Vormetric 2016 Cloud Adoption Report*

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

Por que você deve se preocupar?



Onde os ataques ocorrem normalmente?



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)

O **AWS Identity and Access Management (IAM)** permite controlar o acesso a serviços de computação, armazenamento, banco de dados e aplicativos na Nuvem AWS. O IAM pode ser usado para lidar com autenticação e para especificar e aplicar políticas de autorização para que você possa especificar quais usuários podem acessar quais serviços.

O IAM é uma ferramenta que gerencia de maneira centralizada o acesso à execução, configuração, gerenciamento e encerramento de recursos em sua conta da AWS. Ele fornece controle granular sobre o acesso a recursos, incluindo a capacidade de especificar exatamente quais chamadas de **API** o usuário está autorizado a fazer para cada serviço. Independentemente de você usar o Console de Gerenciamento da AWS, a CLI da AWS ou os kits de desenvolvimento de software (SDKs) da AWS, cada chamada para um serviço da AWS é uma chamada de API.

Com o IAM, você pode gerenciar *quais* recursos podem ser acessados por *quem* e *como* esses recursos podem ser acessados. Você pode conceder permissões diferentes a pessoas distintas para recursos variados. Por exemplo, você pode permitir a alguns usuários acesso total ao Amazon EC2, Amazon S3, Amazon DynamoDB, Amazon Redshift e outros serviços da AWS. No entanto, para outros usuários, pode permitir acesso somente leitura a apenas alguns buckets do S3. Da mesma forma, pode conceder permissão a outros usuários para administrar apenas instâncias do EC2 específicas.

Também é possível permitir que alguns usuários acessem apenas as informações de faturamento da conta, mas nada mais.

O IAM é um recurso da sua conta da AWS que é oferecido gratuitamente.

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.

Para entender como usar o IAM para proteger sua conta da AWS, é importante compreender o papel e a função de cada um dos quatro componentes do IAM.

Um **usuário do IAM** é uma pessoa ou aplicativo definido em uma conta da AWS e que deve fazer chamadas de API para produtos da AWS. Cada usuário deve ter um nome exclusivo (sem espaços no nome) na conta da AWS e um conjunto de credenciais de segurança que não seja compartilhado com outros usuários. Essas credenciais são diferentes das credenciais de segurança do usuário raiz da conta da AWS. Cada usuário é definido em uma única conta da AWS.

Um **grupo do IAM** é um conjunto de usuários do IAM. Você pode usar grupos do IAM para simplificar a especificação e o gerenciamento de permissões para vários usuários.

Uma **política do IAM** é um documento que define permissões para determinar o que os usuários podem fazer na conta da AWS. Uma política normalmente concede acesso a recursos específicos e especifica o que o usuário pode fazer com esses recursos. As políticas também podem negar explicitamente o acesso.

Uma **função do IAM** é uma ferramenta para conceder acesso temporário a recursos específicos da AWS em uma conta 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

Autenticação é um conceito básico de segurança da computação: um usuário ou sistema deve primeiro comprovar a identidade. Considere como você se autentica quando vai para o aeroporto e quer passar pela segurança do aeroporto para poder pegar um voo. Nessa situação, você deve apresentar algum tipo de identificação ao oficial de segurança para comprovar sua identidade antes de entrar em uma área restrita. Um conceito semelhante se aplica para a obtenção de acesso aos recursos da AWS na nuvem.

Ao definir um usuário do IAM, você seleciona o tipo de acesso que o usuário tem permissão para usar para acessar os recursos da AWS. Você pode atribuir dois tipos diferentes de acesso aos usuários: acesso programático e acesso ao Console de Gerenciamento da AWS. Também pode atribuir somente acesso programático, somente acesso ao console ou ambos.

Se você conceder **acesso programático**, o usuário do IAM precisará apresentar um **ID de chave de acesso** e uma **chave de acesso secreta** ao fazer uma chamada de API da AWS usando a CLI da AWS, o SDK da AWS ou alguma outra ferramenta de desenvolvimento.

Se você conceder **acesso ao Console de Gerenciamento da AWS**, o usuário do IAM deverá preencher os campos que aparecem na janela de login do navegador. O usuário deve fornecer o ID da conta com 12 dígitos ou o alias da conta correspondente. O usuário também deve inserir o nome de usuário e a senha do IAM. Se a **Multi-Factor Authentication (MFA)** estiver habilitada para o usuário, ele também deverá fornecer um

código de autenticação.

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.

Console de Gerenciamento da AWS

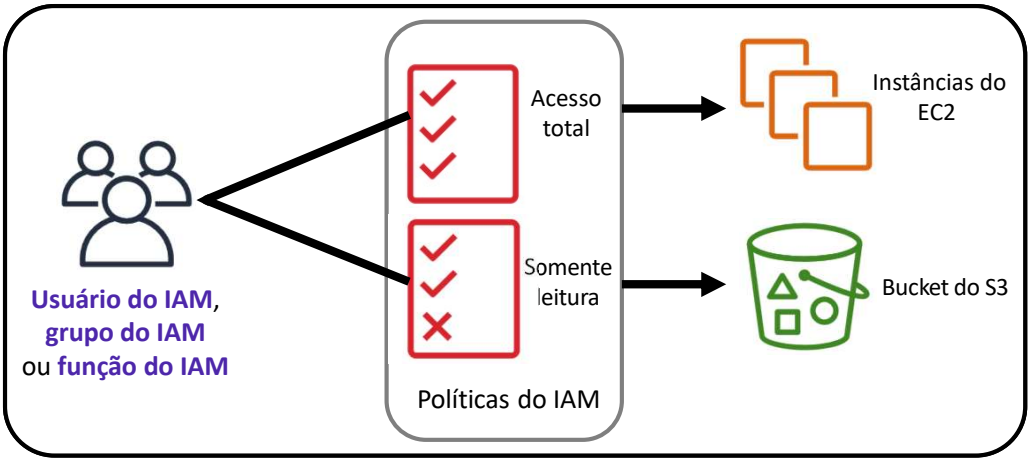
Os serviços e recursos da AWS podem ser acessados com o uso do Console de Gerenciamento da AWS, a CLI da AWS ou por meio de SDKs e APIs. Para maior segurança, recomendamos habilitar a MFA.

Com a MFA, os usuários e os sistemas devem fornecer um **token de MFA** (além das credenciais de login regulares) para que possam acessar os serviços e recursos da AWS.

As opções para gerar o token de autenticação de MFA incluem **aplicativos compatíveis com MFA virtual** (como Google Authenticator ou Authy 2-Factor Authentication), **dispositivos de chave de segurança U2F** e **dispositivos MFA de hardware**.

Autorização: quais ações são permitidas

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



Autorização é o processo de determinar quais permissões um usuário, serviço ou aplicativo deve receber. Depois que um usuário for autenticado, ele deverá ser autorizado a acessar os serviços da AWS.

Por padrão, os usuários do IAM não têm permissões para acessar nenhum recurso ou dados em uma conta da AWS. Em vez disso, você deve conceder permissões explicitamente a um usuário, grupo ou função por meio da criação de uma *política*, que é um documento no formato JavaScript Object Notation (JSON). Uma política lista permissões que permitem ou negam acesso a recursos na conta da AWS.

IAM: autorização

- 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.

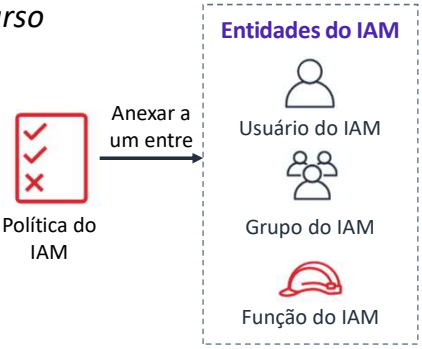
Para atribuir permissão a um usuário, grupo ou função, você deve criar uma **política do IAM** (ou encontrar uma política existente na conta). Não há permissões padrão. Todas as ações na conta são negadas ao usuário por padrão (*negação implícita*), a menos que elas sejam explicitamente permitidas. Qualquer ação que você não permita explicitamente é negada. Todas as ações que você negar explicitamente serão sempre negadas.

O **princípio do privilégio mínimo** é um conceito importante na segurança da computação. Ele consiste em conceder apenas os privilégios mínimos necessários para o usuário, de acordo com as necessidades de seus usuários. Ao criar políticas do IAM, é uma prática recomendada seguir essa orientação de segurança de concessão de *privilégio mínimo*. Determine o que os usuários precisam fazer e, em seguida, crie políticas para eles que permitam que eles executem *apenas* essas tarefas. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Isso é mais seguro do que começar com permissões muito amplas e depois tentar bloquear as permissões concedidas.

O escopo das configurações de serviço do IAM é **global**. As configurações não são definidas no nível da região da AWS. As configurações do IAM se aplicam a todas as regiões da AWS.

Políticas do IAM

- **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)



Uma política do IAM é uma declaração formal de permissões que serão concedidas a uma entidade. As políticas podem ser anexadas a qualquer entidade do IAM. As entidades incluem usuários, grupos, funções ou recursos. Por exemplo, você pode anexar uma política aos recursos da AWS que bloquearão todas as solicitações que não vierem de um intervalo de endereços IP (Internet Protocol) aprovado. As políticas especificam quais ações são permitidas, em quais recursos permitir as ações e qual será o efeito quando o usuário solicitar acesso aos recursos.

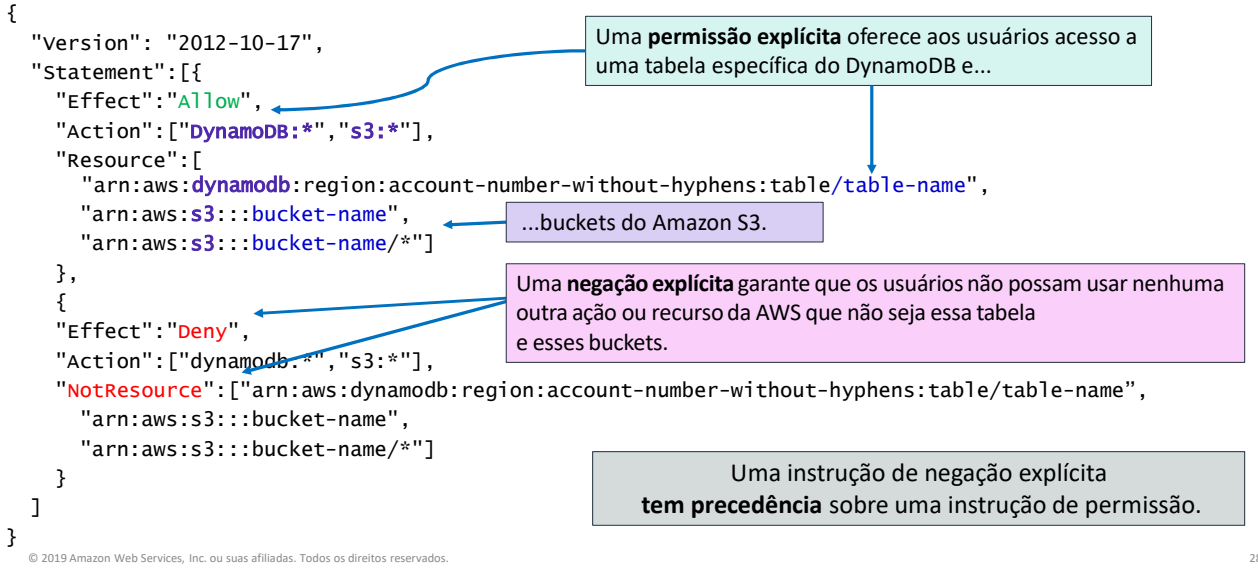
A ordem em que as políticas são avaliadas não tem efeito no resultado da avaliação. Todas as políticas são avaliadas, e o resultado é sempre que a solicitação é permitida ou negada. Quando há um conflito, a política mais restritiva se aplica.

Há dois tipos de políticas do IAM. As **políticas baseadas em identidade** são políticas de permissões que você pode anexar a uma entidade principal (ou identidade), como um usuário, função ou grupo do IAM. Essas políticas controlam quais ações essa identidade pode realizar, em quais recursos e em que condições. As políticas baseadas em identidade podem ser categorizadas como:

- **Políticas gerenciadas:** políticas independentes baseadas em identidade que você pode anexar a vários usuários, grupos e funções em sua conta da AWS
- **Políticas em linha:** políticas que você cria e gerencia e que são incorporadas diretamente em um único usuário, grupo ou função.

As **políticas baseadas em recursos** são documentos de política JSON que você anexa a um recurso, como um bucket do S3. Essas políticas controlam quais ações uma entidade principal pode realizar nesse recurso e em que condições.

Exemplo de política do IAM



Como mencionado anteriormente, os documentos de política do IAM são escritos em JSON.

O exemplo de política do IAM concede aos usuários acesso apenas aos seguintes recursos:

- A tabela do DynamoDB cujo nome é representado por *table-name*.
- O bucket do S3 da conta da AWS, cujo nome é representado por *bucket-name*, e todos os objetos que ela contém.

A política do IAM também inclui um elemento de negação explícita ("Effect":"Deny"). O elemento **NotResource** ajuda a garantir que os usuários não possam usar nenhuma outra ação ou recurso do DynamoDB ou do S3, exceto os especificados na política, mesmo que as permissões tenham sido concedidas em outra política. Uma instrução de negação explícita tem precedência sobre uma instrução de permissão.

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

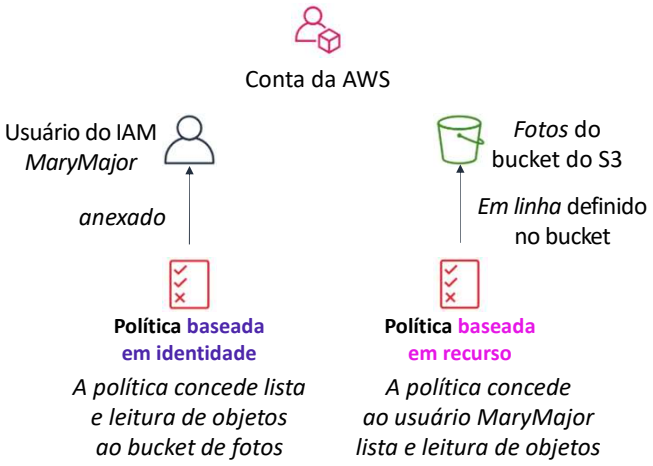
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "elasticloadbalancing:Describe*",
      "Resource": "*"
    },
]
}
```

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



Embora as *políticas baseadas em identidade* estejam anexadas a um usuário, um grupo ou uma função, as **políticas baseadas em recursos** são anexadas a um recurso, como um bucket do S3. Essas políticas especificam quem pode acessar o recurso e quais ações podem ser executadas nele.

As políticas baseadas em recursos são definidas somente **em linha**, o que significa que você define a política no próprio recurso, em vez de criar um documento de política do IAM separado que você anexa. Por exemplo, para criar uma política de bucket do S3 (um tipo de política baseada em recursos) em um bucket do S3, navegue até o bucket, clique na guia **Permissions (Permissões)**, clique no botão **Bucket Policy (Política de bucket)** e defina o documento de política formatado em JSON. Uma lista de controle de acesso (ACL) do Amazon S3 é outro exemplo de uma política baseada em recursos.

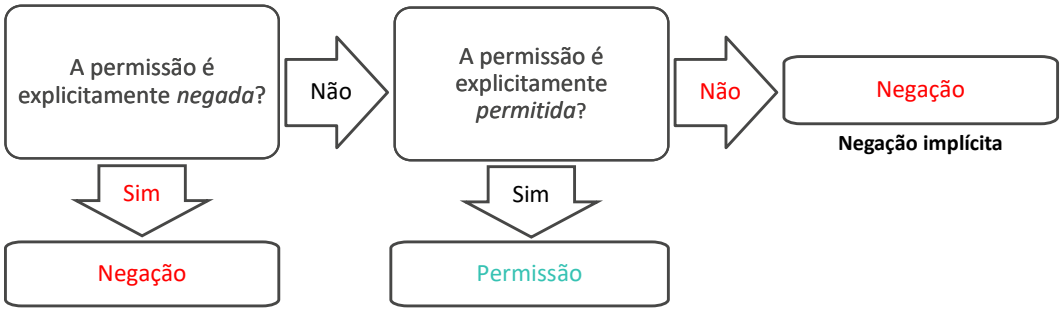
O diagrama mostra duas maneiras diferentes de conceder ao usuário *MaryMajor* acesso a objetos no bucket do S3 chamado *photos*. À esquerda, você vê um exemplo de uma política baseada em identidade. Uma política do IAM que concede acesso ao bucket do S3 é anexada ao usuário MaryMajor. À direita, você vê um exemplo de uma política baseada em recursos. A política de bucket do S3 para o bucket *photos* especifica que o usuário MaryMajor tem permissão para listar e ler os objetos no bucket.

Você pode definir uma instrução de negação em uma política de bucket para restringir o

acesso a usuários específicos do IAM, mesmo que os usuários tenham acesso em uma política separada baseada em identidade. Uma instrução de negação explícita sempre terá precedência sobre qualquer instrução de permissão.

Permissões do IAM

Como o IAM determina permissões:



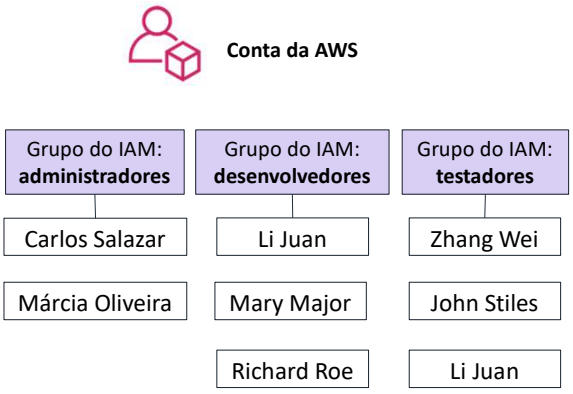
As políticas do IAM permitem ajustar privilégios que são concedidos a usuários, grupos e funções do IAM.

Quando o IAM determina se uma permissão é permitida, ele primeiro verifica a existência de qualquer **política de negação explícita** aplicável. Se não houver uma negação explícita, ele verificará se há alguma **política de permissão explícita** aplicável. Se não houver uma política de negação explícita nem uma de permissão explícita, o IAM reverterá para o padrão, que é negar o acesso. Esse processo é chamado de **negação implícita**. O usuário terá permissão para realizar a ação somente se a ação solicitada *não* for explicitamente negada e *for* explicitamente permitida.

Pode ser difícil descobrir se o acesso a um recurso será concedido a uma entidade do IAM quando você desenvolver políticas do IAM. O Simulador de políticas do IAM é uma ferramenta útil para testar e solucionar problemas de políticas do IAM.

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



Um **grupo do IAM** é um conjunto de usuários do IAM. Os grupos do IAM oferecem uma maneira prática de especificar permissões para um conjunto de usuários, o que pode facilitar o gerenciamento das permissões para esses usuários.

Por exemplo, você pode criar um grupo do IAM chamado *Desenvolvedores* e anexar uma ou várias políticas do IAM a esse grupo que concedem as permissões de acesso a recursos da AWS de que os desenvolvedores geralmente precisam. Qualquer usuário que você adicionar ao grupo Desenvolvedores terá automaticamente as permissões atribuídas ao grupo. Nesse caso, você não precisa anexar as políticas do IAM diretamente ao usuário. Se um novo usuário ingressa em sua organização e precisa receber privilégios de desenvolvedor, você pode simplesmente adicioná-lo ao grupo Desenvolvedores. Da mesma forma, se uma pessoa muda de função em sua organização, em vez de editar as permissões desse usuário, basta removê-lo do grupo.

Características importantes dos grupos do IAM:

- Um grupo pode conter vários usuários, e um usuário pode pertencer a vários grupos.
- Os grupos não podem ser aninhados. Um grupo pode conter apenas usuários, não outros grupos.
- Não há um grupo padrão que inclua automaticamente todos os usuários na conta da AWS. Se você quiser ter um grupo com todos os usuários da conta, precisará criar o grupo e adicionar cada novo usuário a ele.

Funções do IAM

- 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

Uma **função do IAM** é uma identidade do IAM que você pode criar em sua conta que tenha permissões específicas. Uma função do IAM é **semelhante a um usuário do IAM** porque também é uma identidade da AWS à qual você pode anexar políticas de permissões, e essas permissões determinam o que a identidade pode e não pode fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumida por qualquer pessoa que precisar. Além disso, uma função não tem credenciais de longo prazo padrão, como uma senha ou chaves de acesso, associadas a ela. Em vez disso, quando você assume uma função, ela fornece credenciais de segurança temporárias para a sessão da função.

Você pode **usar funções para delegar acesso a usuários, aplicativos ou serviços** que normalmente não têm acesso aos seus recursos da AWS. Por exemplo, você pode conceder aos usuários em sua conta da AWS acesso a recursos que normalmente eles não têm ou conceder aos usuários em uma conta da AWS acesso a recursos em outra conta. Também pode permitir que um aplicativo móvel use recursos da AWS, mas não incorporar chaves da AWS no aplicativo (quando for difícil alterá-las e quando os usuários poderão extraí-las e usá-las indevidamente). Além disso, às vezes você deseja conceder acesso à AWS a usuários que já têm identidades definidas fora da AWS, como no diretório corporativo. Você também pode conceder acesso à sua conta a terceiros, para que eles possam realizar uma auditoria em seus recursos.

Para todos esses exemplos de casos de uso, as funções do IAM são um componente

essencial para a implantação da nuvem.

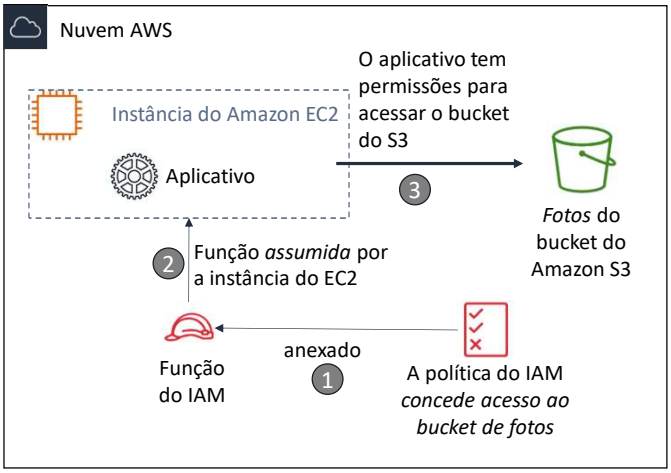
Exemplo de uso de uma função do IAM

Cenário:

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

Solução:

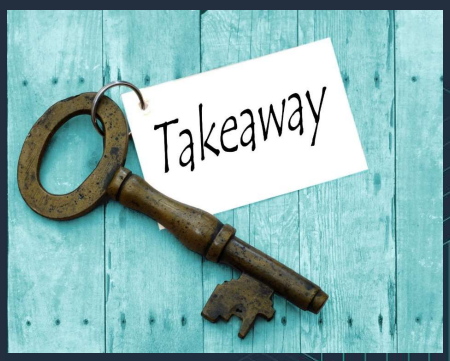
- Defina uma política do IAM que conceda acesso ao bucket do S3.
- Anexe a política a uma função
- Permita que a instância do EC2 assuma a função



No diagrama, um desenvolvedor executa um aplicativo em uma instância do EC2 que requer acesso ao bucket do S3 chamado *photos*. Um administrador cria a função do IAM e anexa a função à instância do EC2. A função inclui uma política de permissões que concede acesso somente leitura ao bucket do S3 especificado. Ele também inclui uma política de confiança que permite que a instância do EC2 assuma a função e recupere as credenciais temporárias. Quando o aplicativo é executado na instância, ele pode usar as credenciais temporárias da função para acessar o bucket **photos**. O administrador não precisa conceder ao desenvolvedor do aplicativo permissão para acessar o bucket photos, e o desenvolvedor nunca precisa compartilhar ou gerenciar credenciais.

Para saber mais detalhes sobre este exemplo, consulte Uso de uma função do IAM para conceder permissões a aplicativos em execução em instâncias do Amazon EC2.

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.

Algumas das principais lições desta seção do módulo são:

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.

Agora, assista à demonstração do IAM. A gravação tem pouco mais de quatro minutos e reforça muitos dos conceitos que foram discutidos nesta seção do módulo.

Veja como configurar os recursos a seguir usando o Console de Gerenciamento da AWS nesta demonstração:

- Uma função do IAM que será usada por uma instância do EC2
- Um grupo do IAM
- Um usuário do IAM

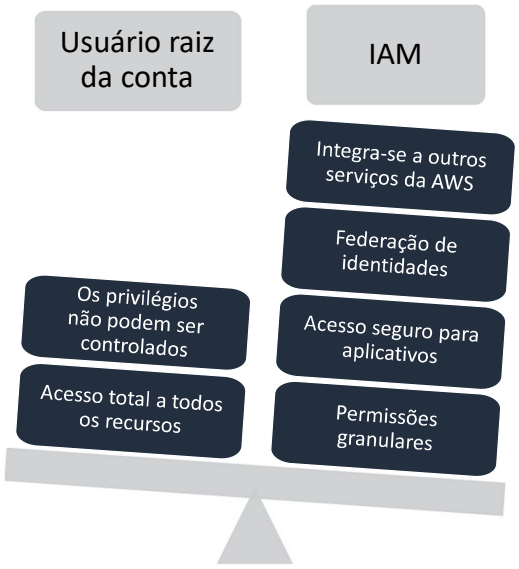
Módulo 4: Segurança na Nuvem AWS

Seção 3: Proteção de uma nova conta da AWS

aws academy

Apresentação da 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)

Ao criar uma conta da AWS pela primeira vez, você começa com uma única identidade de login que tem acesso completo a todos os serviços e recursos da AWS na conta. Essa identidade é chamada de **usuário raiz da conta da AWS** e é acessada por meio de um login no Console de Gerenciamento da AWS com o endereço de e-mail e a senha usados para criar a conta. Os usuários raiz da conta da AWS têm (e mantêm) acesso ***total*** a todos os recursos na conta. Portanto, a AWS recomenda enfaticamente que você não use as credenciais de usuário raiz da conta para interações do dia a dia com a conta.

Em vez disso, a AWS recomenda usar o IAM para criar usuários adicionais e atribuir permissões a eles, seguindo o princípio do privilégio mínimo. Por exemplo, se você precisar de permissões no nível de administrador, poderá criar um usuário do IAM, conceder a ele acesso total e, em seguida, usar essas credenciais para interagir com a conta. Posteriormente, se você precisar revogar ou modificar suas permissões, poderá excluir ou modificar todas as políticas associadas a esse usuário do IAM.

Além disso, se você tiver vários usuários que exigem acesso à conta, poderá criar credenciais exclusivas para cada usuário e definir qual usuário terá acesso a quais recursos. Por exemplo, você pode criar usuários do IAM com acesso somente leitura a recursos em sua conta da AWS e distribuir essas credenciais para usuários que exigem acesso de leitura. Evite compartilhar as mesmas credenciais com vários usuários.

Embora o usuário raiz da conta não deva ser usado para tarefas rotineiras, há algumas

tarefas que só podem ser realizadas fazendo login como o usuário raiz da conta. Uma lista completa dessas tarefas é detalhada na página de documentação Tarefas da AWS que exigem credenciais de usuário raiz da conta da AWS.

Proteção de novas contas da AWS: usuário raiz da conta

aws academy

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.

Para parar de usar o usuário raiz da conta, siga as seguintes etapas:

1. Enquanto você estiver conectado ao usuário raiz da conta, crie um usuário do IAM para você mesmo com o acesso ao Console de Gerenciamento da AWS habilitado (mas não anexe permissões ao usuário ainda). Salve as chaves de acesso do usuário do IAM, se necessário.
2. Em seguida, crie um grupo do IAM, atribua um nome a ele (como *FullAccess*) e anexe políticas do IAM ao grupo que concedam acesso total a pelo menos alguns dos serviços que você usará. Em seguida, 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 todos os usuários. Copie o **link de login de usuários do IAM** na página IAM Dashboard (Painel do IAM). Em seguida, desconecte-se como usuário raiz da conta.
5. Navegue até o link de login de usuários do IAM que você copiou e faça login na conta usando as novas credenciais de usuário do IAM.
6. Armazene as credenciais de usuário raiz da sua conta em um local seguro.

Para ver instruções detalhadas sobre como configurar seu primeiro usuário e grupo do IAM, consulte Criação do primeiro usuário administrador e grupo de administradores do IAM.

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

Outra etapa recomendada para proteger uma nova conta da AWS é exigir Multi-Factor Authentication (MFA) para o login do usuário raiz da conta e para todos os outros logins de usuário do IAM. Você também pode usar a MFA para controlar o acesso programático. Para ver detalhes, consulte Configuração do acesso à API protegido por MFA.

Você tem algumas opções para recuperar o token de MFA necessário para fazer login quando a MFA está habilitada. As opções incluem aplicativos compatíveis com MFA virtual (como Google Authenticator e Authy Authenticator), dispositivos de chave de segurança U2F e opções de MFA de hardware que fornecem um chaveiro ou cartão de exibição.

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).

O AWS CloudTrail é um serviço que registra todas as solicitações de API para recursos na sua conta. Dessa forma, ele permite uma auditoria operacional em sua conta.

Por padrão, o AWS CloudTrail é habilitado na criação de contas em todas as contas da AWS e mantém um registro dos últimos 90 dias de atividades de eventos de gerenciamento de contas. Você pode visualizar e fazer download dos últimos 90 dias de atividade da sua conta para *criar*, *modificar* e *excluir* operações de serviços compatíveis com o CloudTrail sem a necessidade de criar manualmente outra trilha.

Para habilitar a retenção de logs do CloudTrail além dos últimos 90 dias e habilitar alertas sempre que ocorrerem eventos específicos, crie uma nova trilha (que é descrita em um nível superior no slide). Para obter instruções detalhadas sobre como criar uma trilha no AWS CloudTrail, consulte Criação de uma trilha na documentação da AWS.

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.

Uma etapa recomendada adicional para proteger uma nova conta da AWS é habilitar relatórios 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 fornece os relatórios para um bucket do Amazon S3 especificado por você e atualiza os relatórios pelo menos uma vez por dia.

O relatório de custos e uso da AWS monitora o uso na conta da AWS e fornece cobranças estimadas, por hora ou por dia.

Consulte a documentação da AWS para obter detalhes sobre Como criar um relatório de custos e uso da AWS.

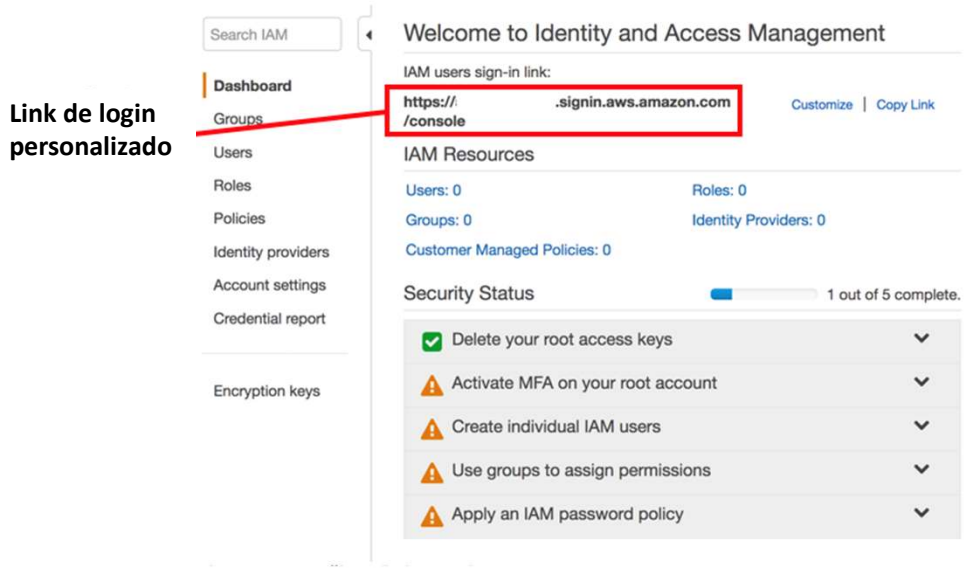
Módulo 4: Segurança na Nuvem AWS

Opcional: Proteção de novas contas da AWS – demonstração completa

aws academy

O instrutor também pode optar por mostrar uma demonstração completa das duas primeiras etapas principais que você deve concluir para proteger uma nova conta da AWS. (Essas etapas foram descritas nos slides anteriores.) Os slides desta seção fornecem capturas de tela de como é passar pelo processo em detalhes.

Análise do status de segurança do IAM



A captura de tela mostra um exemplo da aparência do painel do console do IAM quando você está conectado como usuário raiz da conta da AWS. Para acessar essa tela em uma conta:

1. Faça login no **Console de Gerenciamento da AWS** como usuário raiz da conta da AWS.
2. Acesse a página de serviço do **IAM** e clique no link **Dashboard (Painel)**.
3. Revise as informações no painel **Security Status (Status de segurança)**.

Na captura de tela, apenas uma das cinco verificações de status de segurança foi concluída (*Delete your root access keys [Excluir suas chaves de acesso raiz]*). O objetivo de uma pessoa que conclui as etapas para proteger a conta é receber marcas de seleção verdes ao lado de cada item de status de segurança.

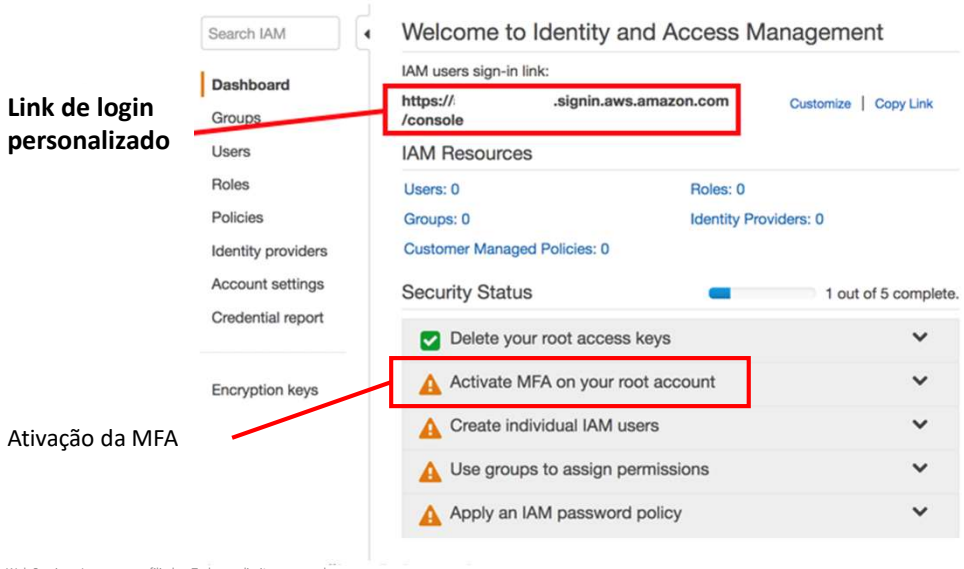
Uma revisão da lista atual **Security Status (Status de segurança)** indica que:

- A MFA *não* foi ativada no usuário raiz da conta da AWS.
- Nenhum usuário individual do IAM foi criado.
- Nenhuma permissão foi atribuída a grupos.

- Nenhuma política de senha do IAM foi aplicada.

Há um link de login de usuário do IAM personalizado para a conta. O número da conta foi ocultado nesta captura de tela. Como opção, você pode usar o link **Customize (Personalizar)** à direita do link de login de usuário do IAM para alterar o nome da conta para que ela não exiba o número da conta. Esse link é usado para fazer login na conta e pode ser enviado aos usuários depois que as contas deles forem criadas.

Ative a MFA no usuário raiz da conta

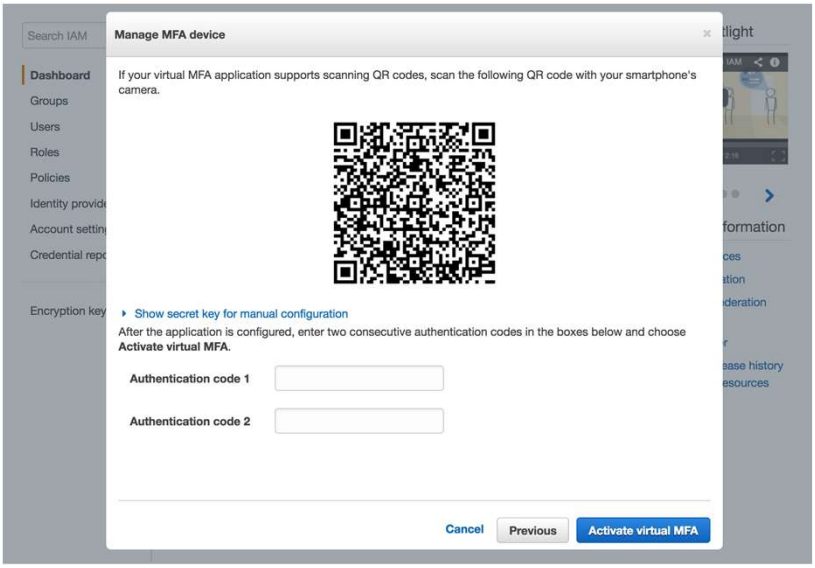


Antes de criar usuários do IAM na conta, ative a MFA no usuário raiz da conta. Para fazer login como usuário raiz da conta, use o endereço de e-mail usado para criar a conta. O usuário raiz da conta tem acesso a tudo, e é por isso que é importante proteger essa conta com restrições.

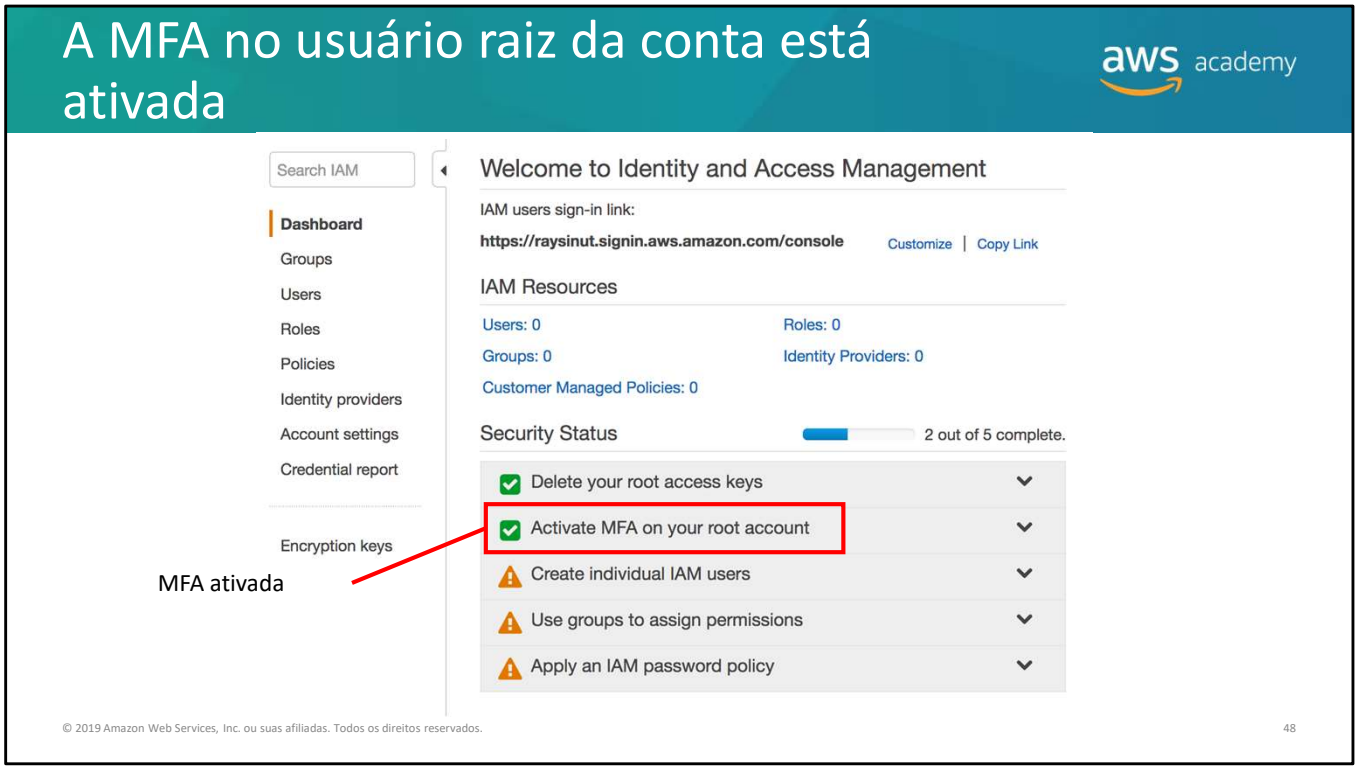
Para configurar a MFA:

1. Clique no link **Activate MFA on your root account (Ativar MFA na sua conta raiz)**.
2. Clique em **Manage MFA (Gerenciar MFA)**.
3. Clique em **Assign MFA device (Atribuir dispositivo MFA)**. Você tem três opções: **Virtual MFA device (Dispositivo MFA virtual)**, **U2F security key (Chave de segurança U2F)** e **Other hardware MFA device (Outro dispositivo MFA de hardware)**. Um dispositivo de hardware é um dispositivo de hardware real.
4. Para esta demonstração, selecione **Virtual MFA device (Dispositivo MFA virtual)** e clique em **Continue (Continuar)**.
5. Uma nova caixa de diálogo é exibida e pede que você configure um dispositivo MFA virtual. Um aplicativo (como o Google Authenticator) deve ser baixado para realizar essa tarefa. Após a conclusão do download, clique em **Show QR code (Mostrar código QR)**.

Ative a MFA no usuário raiz da conta



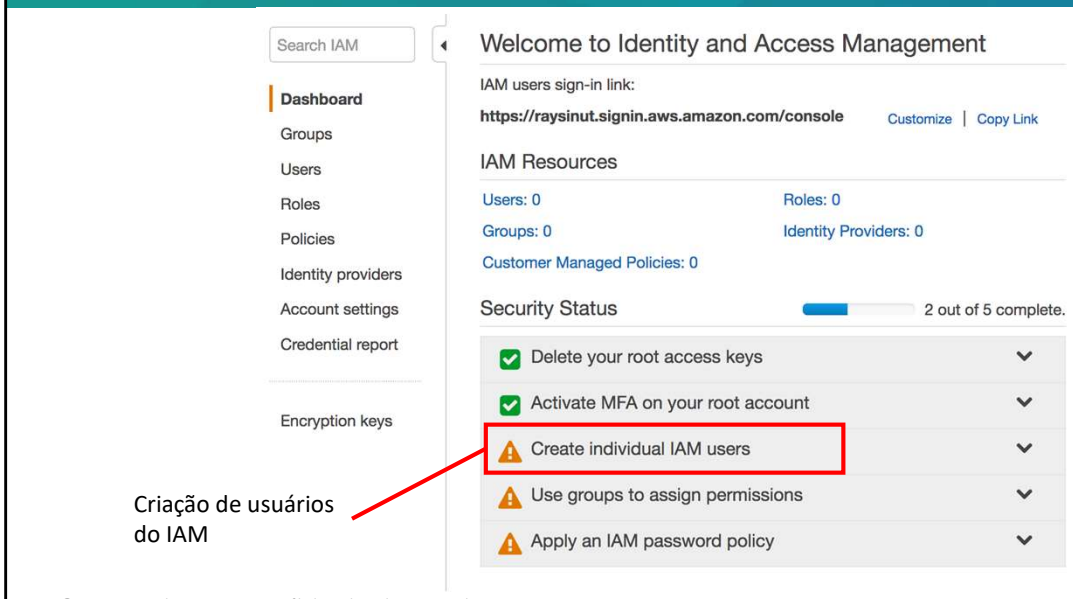
6. No aplicativo autenticador, escolha o **sinal de adição (+)**.
7. Digitalize o código de barras e insira o primeiro código de autenticação.
8. Aguarde um momento para que o segundo código seja exibido e o insira.
9. Clique no botão **Assign MFA (Atribuir MFA)**.



10. Clique em **Finish (Concluir)** e atualize seu navegador.

O painel **Security Status (Status de segurança)** agora deve mostrar um ícone de marca de seleção verde, o que indica que a MFA está ativada no usuário raiz da conta.

Crie um usuário do IAM individual (1)



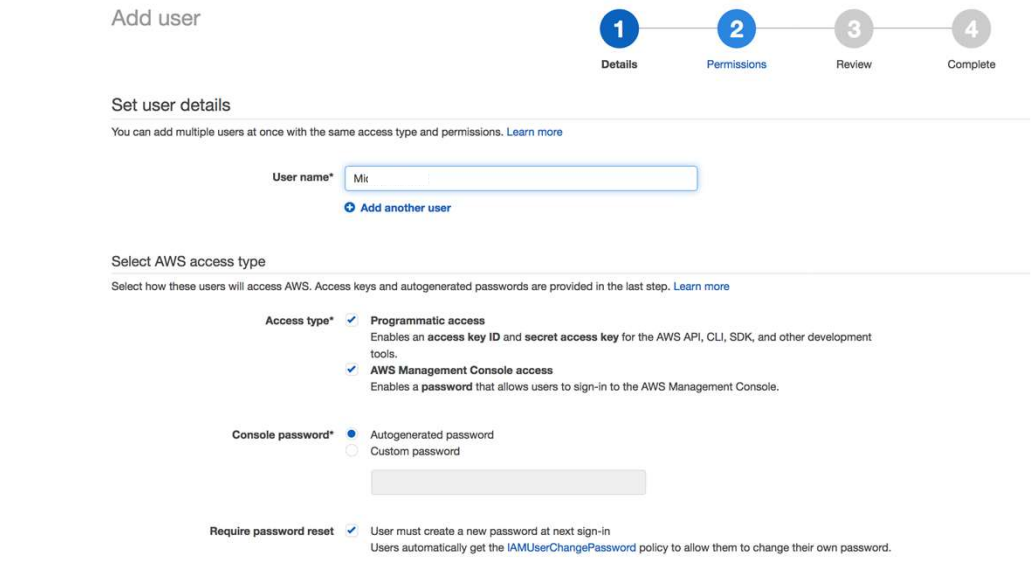
A maioria das contas da AWS são compartilhadas por vários usuários em uma organização. Para oferecer suporte a essa prática, você pode configurar cada usuário com permissões atribuídas individualmente ou adicionar usuários ao grupo do IAM apropriado que concede permissões específicas a eles.

Uma prática recomendada da AWS é fornecer a cada usuário o próprio login de usuário do IAM para que ele não faça login como usuário raiz da conta com privilégios globais ou use as mesmas credenciais de outra pessoa para fazer login na conta.

Para configurar essa configuração:

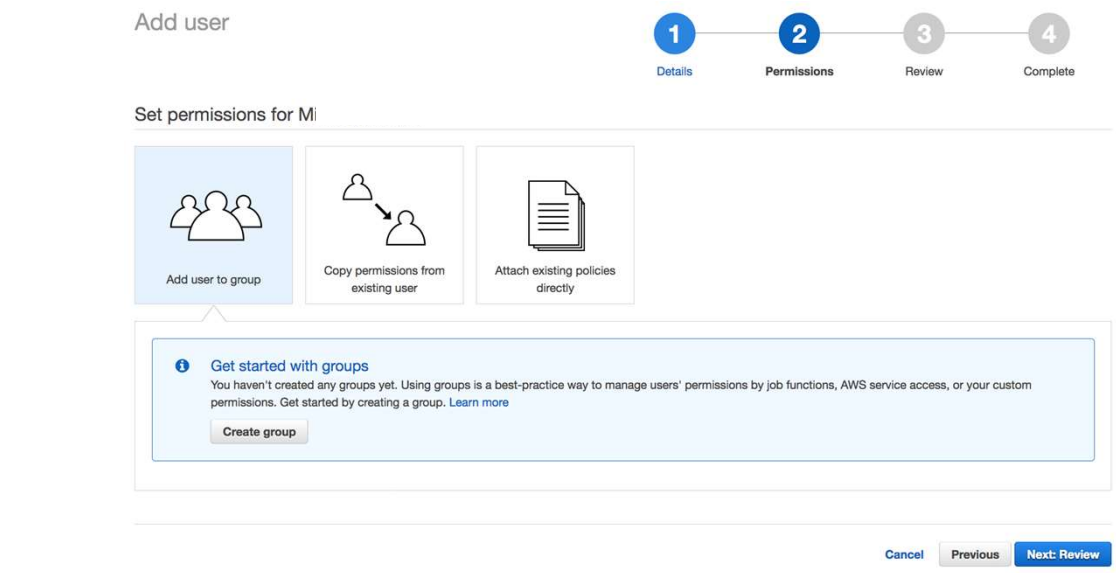
1. Clique em **Create individual IAM users (Criar usuários individuais do IAM)** e selecione **Manage Users (Gerenciar usuários)**.

Crie um usuário do IAM individual (2)



2. Selecione **Add user (Adicionar usuário)** e especifique um novo nome de usuário. Os nomes de usuário não podem ter espaços.
3. Selecione o **Access type (Tipo de acesso)**. Há dois tipos de acesso (você pode conceder um tipo ou ambos ao usuário, mas, para esta demonstração, conceda os dois):
    - **acesso programático** permite que o usuário tenha acesso à CLI da AWS para provisionar recursos. Essa opção gerará uma chave de acesso uma vez. Essa chave de acesso deve ser salva porque será usada para todos os acessos futuros.
    - **acesso ao Console de Gerenciamento da AWS** permite que o usuário faça login no console.
4. Se você optar por conceder acesso ao console, escolha **Autogenerate password (Gerar senha automaticamente)** ou selecione **Custom password (Senha personalizada)** e insira uma.
5. Clique em **Next: Permissions (Próximo: Permissões)**.

Crie um usuário do IAM individual (3)



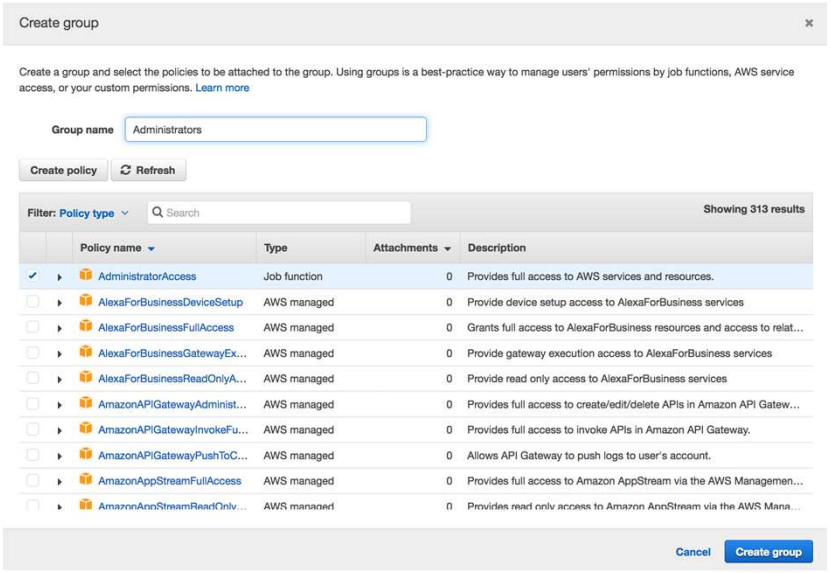
Em seguida, você atribuirá permissões. Você tem três opções para atribuir permissões:

- Adicionar usuário ao grupo
- Copiar permissões de um usuário existente
- Anexar políticas existentes diretamente

6. Você quer adicionar o usuário a um grupo; portanto, selecione **Add user to group (Adicionar usuário ao grupo)** e escolha **Create group (Criar grupo)**.

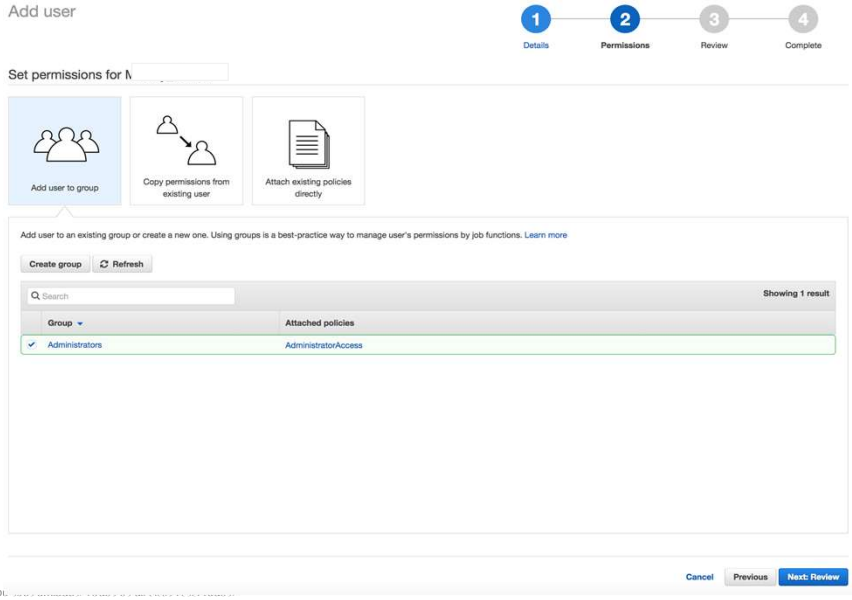
Observação: um grupo é onde você coloca os usuários para herdar as políticas atribuídas ao grupo.

Crie um usuário do IAM individual (4)



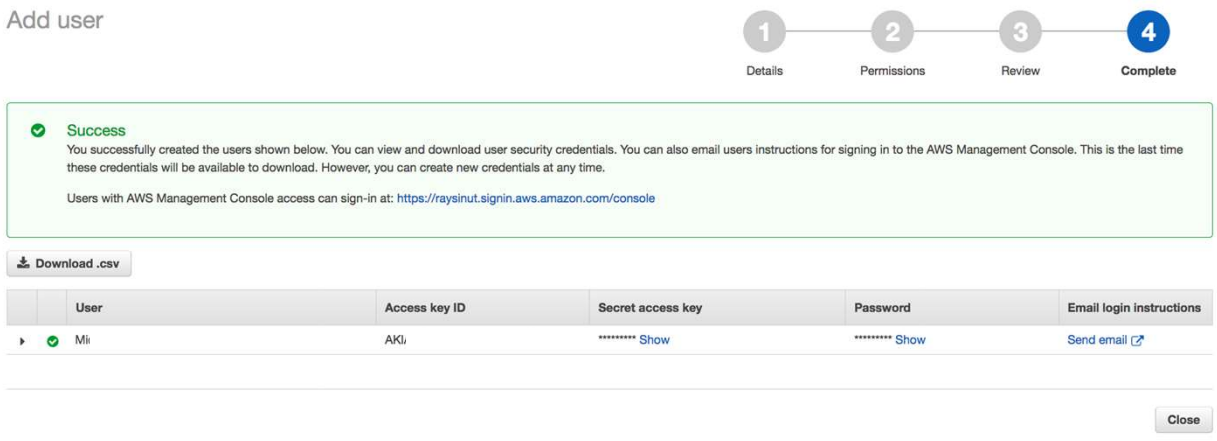
7. Dê um nome para o grupo. Neste exemplo, conceda ao desenvolvedor principal acesso administrativo e escolha **Create group (Criar grupo)**.

Crie um usuário do IAM individual (5)



8. Selecione **Next Review (Próxima revisão)** para revisar o que será criado e escolha **Create user (Criar usuário)**.

Criação de usuário do IAM bem-sucedida



Quando um usuário é criado (e supondo que você tenha habilitado o acesso programático e ao console ao definir a **Access type (Tipo de acesso)** configuração e criado o usuário), vários artefatos serão gerados:

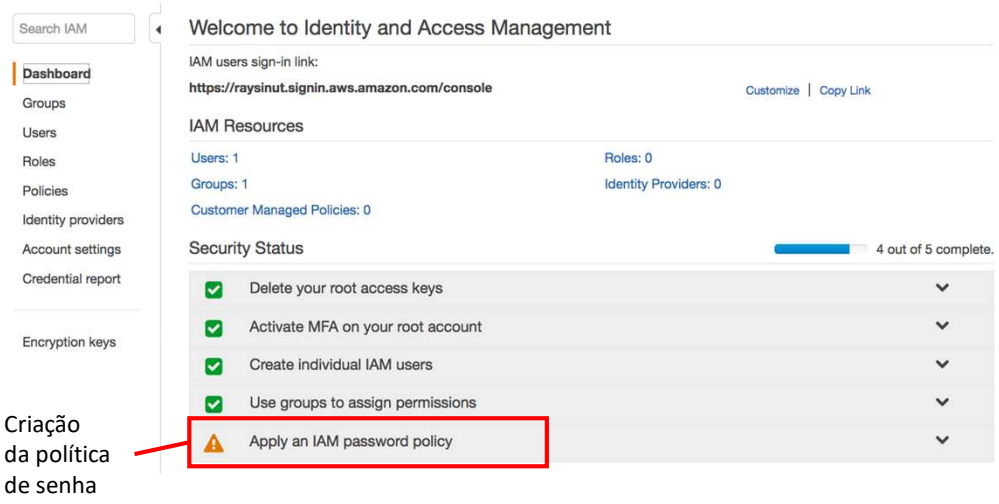
1. Um **ID de chave de acesso** que pode ser usado para assinar chamadas de API da AWS quando o usuário usa a CLI ou os SDKs da AWS.
2. Uma **chave de acesso secreta** que também é usada para assinar chamadas de API da AWS quando o usuário usa a CLI ou os SDKs da AWS.
3. Uma **senha** que pode ser usada para fazer login no Console de Gerenciamento da AWS.

Escolha **Show (Mostrar)** para exibir os valores em cada campo. As credenciais também podem ser baixadas ao escolher **Download .csv (Fazer download do .csv**). Essa é a única vez em que você tem a opção de fazer download dessas credenciais. Você não terá a oportunidade de recuperar a chave de acesso secreta após essa tela. Portanto, faça download das credenciais ou, no mínimo, copie a chave de acesso secreta e cole-a em

um local seguro.

Importante: nunca armazene essas credenciais em um local público (por exemplo, nunca incorpore essas credenciais no código carregado no GitHub ou em outro lugar). Essas informações podem ser usadas para acessar sua conta. Se você tiver a preocupação de que suas credenciais foram comprometidas, faça login como um usuário com permissões de acesso de administrador do IAM e exclua a chave de acesso existente. Em seguida, crie uma nova chave de acesso.

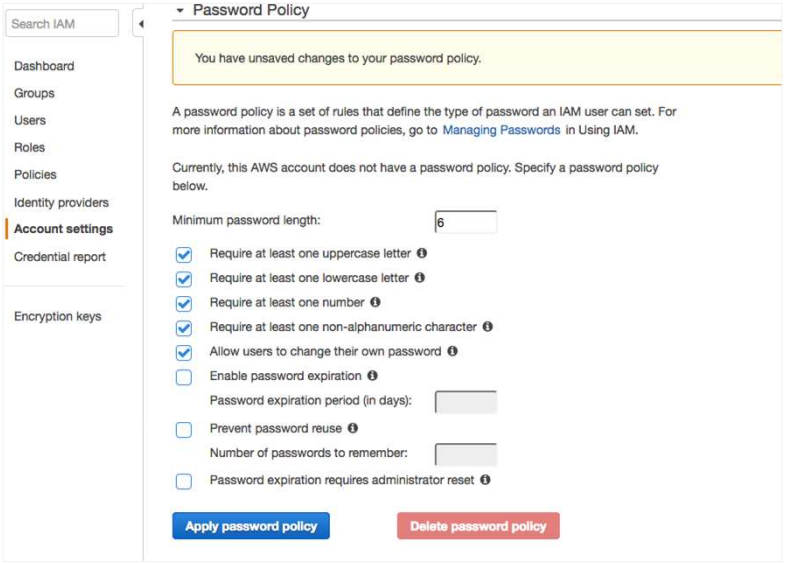
Status de segurança do painel do IAM



Quando você retornar ao Painel do IAM, os itens de status de segurança **Create individual IAM users (Criar usuários individuais do IAM)** e **Use groups to assign permissions (Usar grupos para atribuir permissões)** devem mostrar que foram abordados.

O item de segurança restante a ser abordado é a aplicação de uma política de senha do IAM.

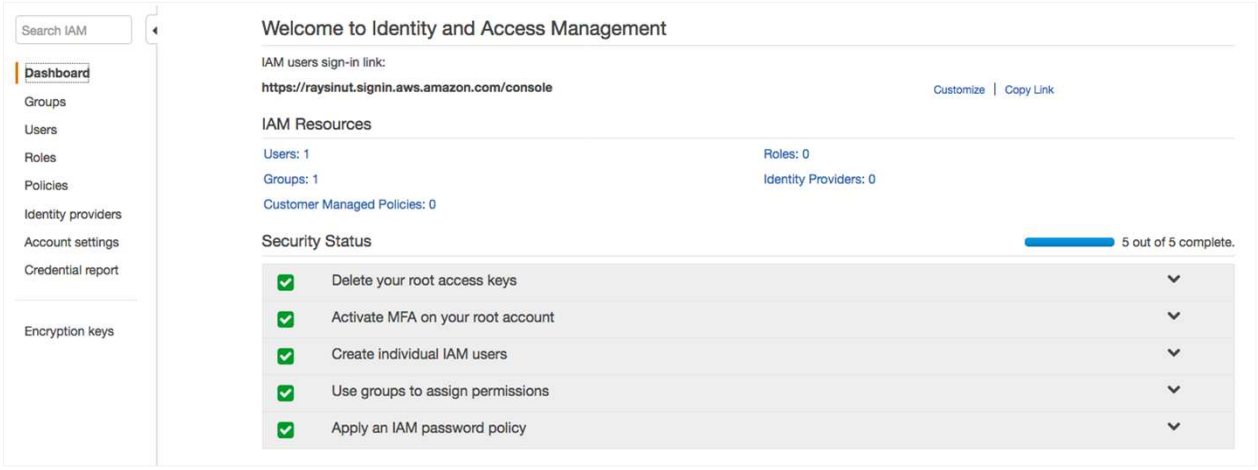
Defina uma política de senhas do IAM



A política de senha do IAM é um conjunto de regras que define o tipo de senha que um usuário do IAM pode configurar.

Selecione as regras com as quais as senhas devem estar em conformidade e escolha **Apply password policy (Aplicar política de senha)**.

Verificações de status de segurança concluídas



Todas as marcas de verificação de status de segurança agora devem estar verdes. Sua conta agora está em conformidade com as verificações de status de segurança do IAM listadas. Parabéns!

Principais lições da Seção 3

aws academy

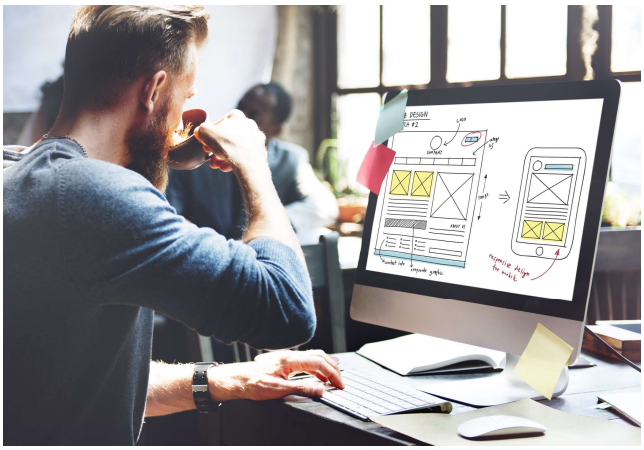
Práticas recomendadas para proteger uma conta da AWS:

- **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.

As principais lições desta seção do módulo estão todas relacionadas às práticas recomendadas para proteger uma conta da AWS. Essas recomendações incluem:

- 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



Introdução ao laboratório 1: Introdução ao AWS IAM.

Laboratório 1: Tarefas

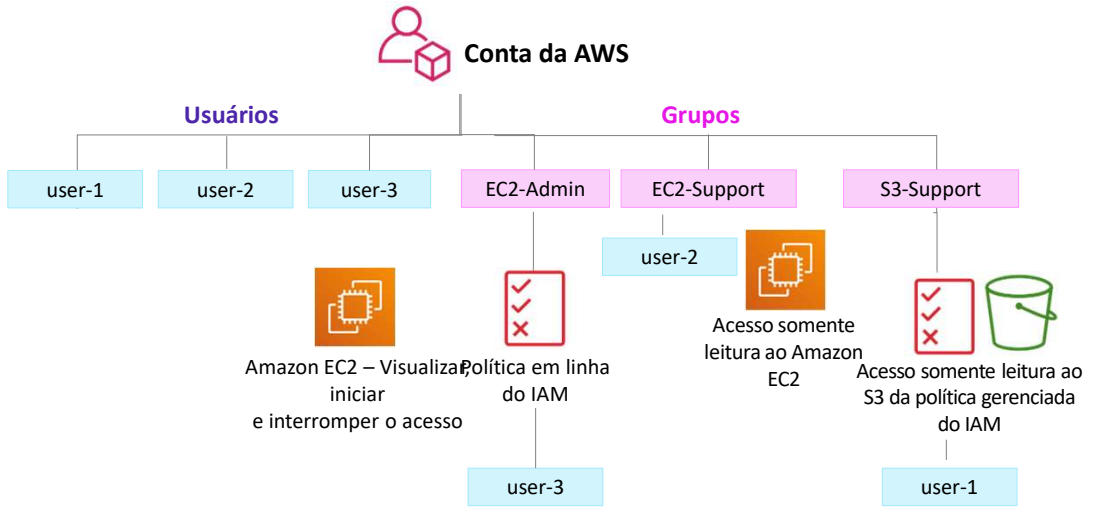
- Tarefa 1: explorar usuários e grupos.
- Tarefa 2: adicionar usuários aos grupos.
- Tarefa 3: fazer login e testar usuários.

AWS Identity and
Access Management (IAM)

Neste laboratório prático, você vai:

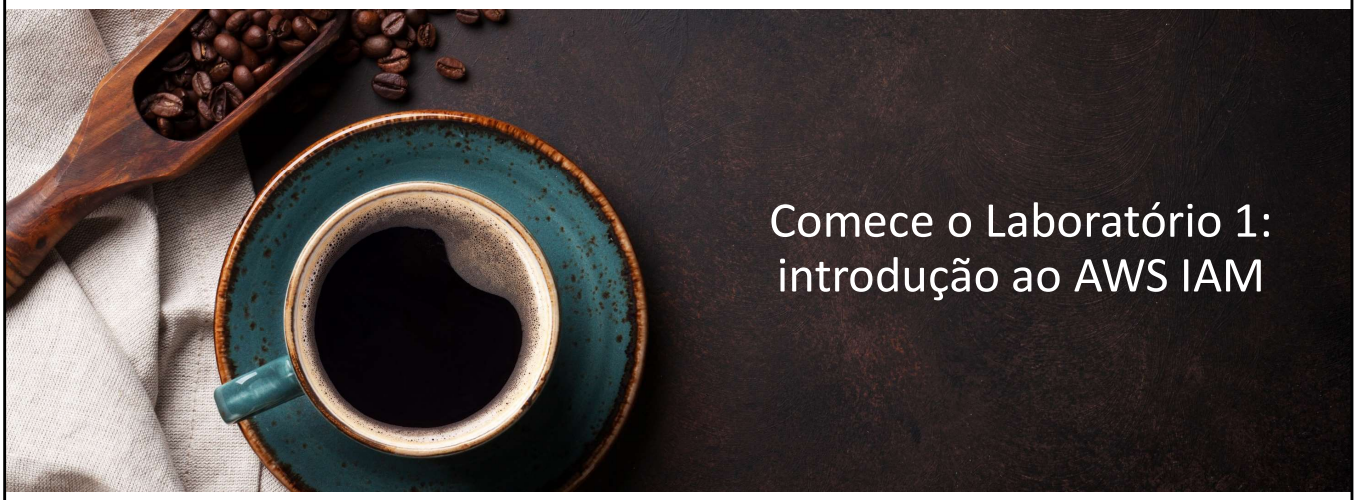
- Explorar usuários e grupos do IAM pré-criados.
- Inspecionar as políticas do IAM à medida que são aplicadas aos grupos pré-criados.
- Seguir um cenário real e adicionar usuários a grupos com recursos específicos habilitados.
- Localizar e usar o URL de login do IAM.
- Testar os efeitos das políticas do IAM no acesso aos recursos da AWS.

Laboratório 1: Produto final



O diagrama mostra os recursos que sua conta da AWS terá depois que você concluir as etapas do laboratório. Ele também descreve como os recursos serão configurados.

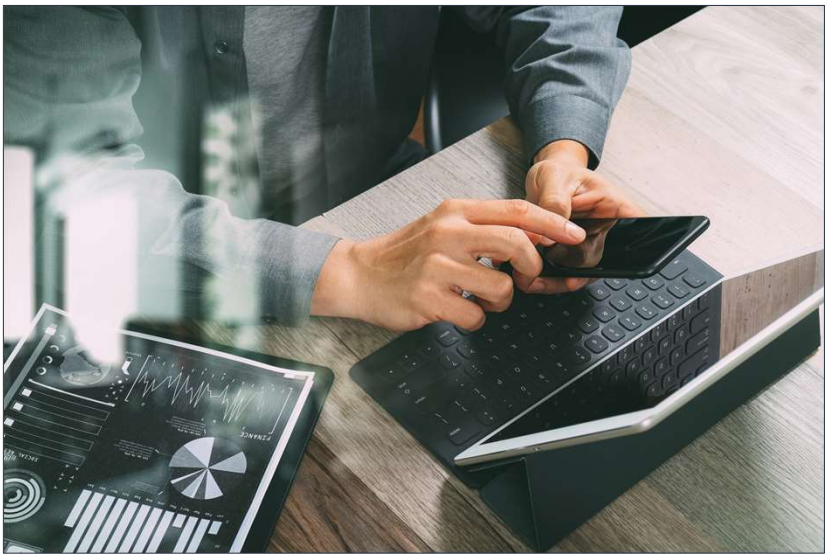
Aproximadamente
40 minutos



Comece o Laboratório 1: introdução ao AWS IAM

Agora é hora de iniciar o laboratório.

Resumo do laboratório: principais lições



O instrutor agora conduzirá uma conversa sobre as principais lições do laboratório depois que você o concluir.

Módulo 4: Segurança na Nuvem AWS

Seção 4: Proteção de contas

aws academy

Apresentação da 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

O **AWS Organizations** é um serviço de gerenciamento de contas que permite consolidar várias contas da AWS em uma *organização* que você cria e gerencia de modo centralizado. Aqui, o foco está nos recursos de segurança que o AWS Organizations oferece.

Um recurso de segurança útil é que você pode **agrupar contas em unidades organizacionais** (OUs) e anexar políticas de acesso diferentes a cada OU. Por exemplo, se você tiver contas que só devem ter permissão para acessar serviços da AWS que atendam a determinados requisitos normativos, poderá colocá-las em uma OU. Em seguida, você pode definir uma política que bloqueie o acesso da OU aos serviços que não atendem a esses requisitos normativos e, em seguida, anexar a política à OU.

Outro recurso de segurança é que o **AWS Organizations se integra ao IAM e é compatível com ele.** O AWS Organizations expande esse controle para o nível da conta, permitindo controlar o que os usuários e as funções de uma conta ou grupo de contas podem fazer. As permissões resultantes são a interseção lógica do que é permitido pelas configurações de política do AWS Organizations e quais permissões são explicitamente concedidas pelo IAM na conta para esse usuário ou essa função. O usuário pode acessar apenas o que é permitido pelas ***duas*** políticas do AWS Organizations e pelas políticas do IAM.

Por fim, o AWS Organizations **fornece políticas de controle de serviço (SCPs)** que permitem especificar o número máximo de permissões que as contas de membro na organização podem ter. Nas SCPs, você pode restringir quais serviços, recursos e ações individuais da AWS os usuários e as funções em cada conta de membro podem acessar. **Essas restrições até substituem os administradores de contas de membro**. Quando o AWS Organizations bloqueia o acesso a um serviço, um recurso ou uma ação de API, um usuário ou uma função nessa conta não poderá acessá-lo, mesmo que um administrador de uma conta de membro explicitamente conceda essas permissões.

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.

Veja a seguir o recurso **políticas de controle de serviço (SCPs)** do AWS Organizations.

As SCPs oferecem controle central sobre o **número máximo de permissões disponíveis** para todas as contas em sua organização, permitindo que você verifique se suas contas permanecem de acordo com as diretrizes de controle de acesso de sua organização. As SCPs estão disponíveis somente em uma organização que tenha todos os recursos habilitados, incluindo o faturamento consolidado. As SCPs não estarão disponíveis se sua organização tiver habilitado *apenas* os recursos de faturamento consolidado. Para obter instruções sobre como habilitar SCPs, consulte Habilitação e desabilitação de um tipo de política em uma raiz.

As **SCPs são semelhantes às políticas de permissões do IAM** e usam praticamente a mesma sintaxe. No entanto, uma SCP nunca concede permissões. Em vez disso, as SCPs são políticas JSON que especificam o número máximo de permissões para uma organização ou OU. Anexar uma SCP à raiz da organização ou a uma unidade organizacional (OU) define uma proteção para as ações que as contas na raiz da organização ou na OU podem realizar. No entanto, isso não substitui as configurações bem gerenciadas do IAM dentro de cada conta. Você ainda deve anexar políticas do IAM a usuários e funções nas contas da sua organização para realmente conceder permissões a eles.

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)

O **AWS Key Management Service (AWS KMS)** é um serviço que permite criar e gerenciar chaves de criptografia e controlar o uso da criptografia em uma grande variedade de serviços da AWS e seus aplicativos. O AWS KMS é um serviço seguro e resiliente que usa módulos de segurança de hardware (HSMs) validados (ou em processo de validação) de acordo com o **Federal Information Processing Standards (FIPS) 140-2** para proteger suas chaves. O AWS KMS também é integrado ao AWS CloudTrail para fornecer logs que contêm toda a utilização das chaves para ajudar a cumprir requisitos normativos e de conformidade.

As **chaves mestras de cliente (CMKs)** são usadas para controlar o acesso às chaves de criptografia de dados que criptografam e descriptografam seus dados. Você pode criar novas chaves mestras quando desejar e gerenciar quem tem acesso a elas e com quais serviços elas podem ser usadas. Também pode importar chaves de sua própria infraestrutura de gerenciamento de chaves para o AWS KMS.

O AWS KMS integra-se à maioria dos serviços da AWS, o que significa que você pode usar as chaves mestras do dele para controlar a criptografia dos dados armazenados nesses serviços. Para saber mais, consulte Recursos do AWS Key Management Service.

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

O Amazon Cognito oferece soluções para controlar o acesso aos recursos da AWS a partir do seu aplicativo. Você pode definir funções e mapear usuários a funções diferentes para que o aplicativo possa acessar apenas os recursos autorizados para cada usuário.

O Amazon Cognito usa padrões comuns de gerenciamento de identidade,como o **Security Assertion Markup Language (SAML) 2.0**. O SAML é um padrão aberto para troca de informações de identidade e segurança com aplicativos e provedores de serviços. Os aplicativos e provedores de serviços compatíveis com o SAML permitem fazer login usando suas credenciais de diretório corporativo, como seu nome de usuário e sua senha do Microsoft Active Directory. Com o SAML, você pode usar o logon único (SSO) para fazer login em todos os seus aplicativos habilitados para SAML usando um único conjunto de credenciais.

O Amazon Cognito ajuda a **cumprir vários requisitos de segurança e conformidade**, incluindo requisitos para organizações altamente regulamentadas, como empresas e vendedores da área da saúde. O Amazon Cognito está qualificado para uso com a Health Insurance Portability and Accountability Act (HIPAA– Lei de portabilidade e responsabilidade do seguro de saúde) dos EUA. Ele também pode ser usado para cargas de trabalho que estejam em conformidade com o Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS); com o Controle de organização de serviço

(SOC) do American Institute of CPAs (AICPA); com os padrões da International Organization for Standardization (ISO) e da International Electrotechnical Commission (IEC) ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018; e ISO 9001.

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

O **AWS Shield** é um serviço gerenciado de proteção contra negação de serviço distribuída (DDoS) que protege aplicativos executados na AWS. Ele fornece detecção e mitigações embutidas automáticas e sempre ativas que minimizam o tempo de inatividade e a latência dos aplicativos. Assim, não é necessário interagir com o AWS Support para ter benefícios de proteção contra DDoS.

O AWS Shield ajuda a proteger seu site contra todos os tipos de ataques DDoS, incluindo ataques na camada de infraestrutura (como floods de User Datagram Protocol, ou UDP), ataques de exaustão de estado (como floods de TCP SYN) e ataques na camada de aplicativos (como floods HTTP GET ou POST). Para ver exemplos, consulte o Guia do desenvolvedor do AWS WAF e do AWS Shield Advanced.

O **AWS Shield Standard** é habilitado automaticamente para todos os clientes da AWS sem custo adicional.

O **AWS Shield Advanced** é um serviço pago opcional. O AWS Shield Advanced oferece proteções adicionais contra ataques maiores e mais sofisticados para aplicativos executados no Amazon EC2, no Elastic Load Balancing, no Amazon CloudFront, no AWS Global Accelerator e no Amazon Route 53. O AWS Shield Advanced está disponível para todos os clientes. No entanto, para entrar em contato com a equipe de resposta a DDoS, os clientes precisam ter o Enterprise Support ou o Business Support do AWS Support.

Módulo 4: Segurança na Nuvem AWS

Seção 5: Proteção de dados na AWS

aws academy

Apresentação da 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

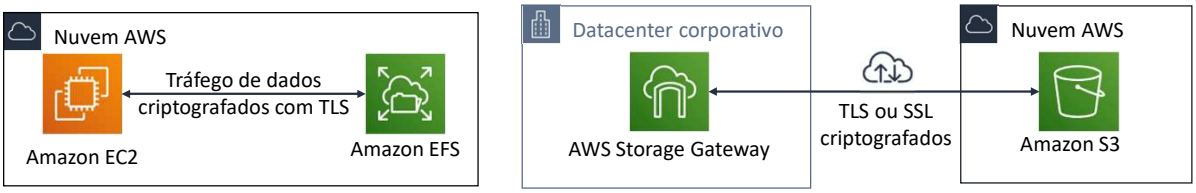
A **criptografia de dados** é uma ferramenta essencial para usar quando seu objetivo é proteger dados digitais. A criptografia de dados usa dados legíveis e os codifica para que não possam ser lidos para nenhuma pessoa que não tenha acesso à chave secreta que pode ser usada para decodificá-los. Portanto, mesmo que um invasor obtenha acesso aos seus dados, eles não servirão para nada.

Dados em repouso referem-se a dados armazenados fisicamente em disco ou em fita.

Você pode criar sistemas de arquivos criptografados na AWS para que todos os seus dados e metadados sejam criptografados em repouso com o uso do algoritmo de criptografia de padrão aberto Advanced Encryption Standard (AES)-256. Quando você usa o AWS KMS, a criptografia e a descriptografia são processadas de maneira automática e transparente para que você não precise modificar seus aplicativos. Se sua organização estiver sujeita a políticas corporativas ou normativas que exigem criptografia de dados e metadados em repouso, a AWS recomenda habilitar a criptografia em todos os serviços que armazenam seus dados. Você pode criptografar dados armazenados em qualquer serviço compatível com o AWS KMS. Consulte Como os serviços da AWS usam o AWS KMS para obter uma lista dos serviços compatíveis.

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:



Dados em trânsito referem-se a dados que se movem pela rede. A criptografia de dados em trânsito é realizada usando o Transport Layer Security (TLS) 1.2 com uma criptografia AES-256 padrão aberto. O TLS antes era chamado de Secure Sockets Layer (SSL).

O **AWS Certificate Manager** é um serviço que permite provisionar, gerenciar e implantar certificados SSL ou TLS para uso com serviços da AWS e os seus recursos internos conectados. Os certificados SSL ou TLS são usados para proteger as comunicações de rede e estabelecer a identidade de sites pela Internet e também recursos em redes privadas. Com o AWS Certificate Manager, você pode solicitar um certificado e implantá-lo em recursos da AWS (como load balancers ou distribuições do CloudFront). O AWS Certificate Manager também processa renovações de certificados.

O tráfego da web executado por HTTP não é seguro. No entanto, o tráfego executado por **HTTP seguro (HTTPS)** é criptografado com TLS ou SSL. O tráfego HTTPS é protegido contra espionagem e ataques man-in-the-middle devido à criptografia bidirecional da comunicação.

Os serviços da AWS oferecem suporte à criptografia de dados em trânsito. Veja a seguir dois exemplos de criptografia para dados em trânsito. O primeiro exemplo mostra uma instância do EC2 que montou um sistema de arquivos compartilhados do Amazon EFS. Todo o tráfego de dados entre a instância e o Amazon EFS é criptografado com TLS ou

SSL. Para obter mais detalhes sobre essa configuração, consulte Criptografia de dados do EFS em trânsito.

O segundo exemplo mostra o uso do **AWS Storage Gateway,** um serviço de armazenamento na nuvem híbrida que fornece acesso local ao armazenamento na Nuvem AWS. Neste exemplo, o storage gateway é conectado pela Internet ao Amazon S3, e a conexão criptografa os dados em trânsito.

Proteção de buckets e objetos do Amazon S3

- 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.

Por padrão, todos os buckets do Amazon S3 são privados e *só* podem ser acessados por usuários que recebem acesso explicitamente concedido. É essencial gerenciar e controlar o acesso aos dados do Amazon S3. A AWS oferece muitas ferramentas e opções para controlar o acesso aos buckets ou objetos do S3, incluindo:

- Uso do **Amazon S3 Block Public Access**. Essas configurações substituem quaisquer outras políticas ou permissões de objeto. Habilite o **Block Public Access** para todos os buckets que você não deseja que sejam acessíveis publicamente. Esse recurso oferece um método simples para evitar a exposição não intencional de dados do Amazon S3.

- Escrita de **políticas do IAM** que especificam os usuários ou as funções que podem acessar buckets e objetos específicos. Esse método foi discutido em detalhes anteriormente neste módulo.

- Escrita de **políticas de bucket** que definem o acesso a buckets ou objetos específicos. Essa opção normalmente é usada quando o usuário ou o sistema não pode autenticar com o IAM. As políticas de bucket podem ser configuradas para conceder acesso entre contas da AWS ou para conceder acesso público ou anônimo aos dados do Amazon S3. Se as políticas de bucket forem usadas, elas deverão ser escritas

cuidadosamente e testadas por completo. Você pode especificar uma instrução de negação em uma política de bucket para restringir o acesso. O acesso será restrito mesmo se os usuários tiverem permissões concedidas em uma política baseada em identidade anexada aos usuários.

- Definição de **listas de controle de acesso (ACLs)** nos buckets e objetos. As ACLs são menos usadas (as ACLs são anteriores ao IAM). Se você usar ACLs, não defina um acesso muito aberto ou permissivo.

- **AWS Trusted Advisor** oferece um recurso de verificação de permissões de bucket que é uma ferramenta útil para descobrir se algum dos buckets em sua conta tem permissões que concedem acesso global.

Módulo 4: Segurança na Nuvem AWS

Seção 6: Trabalhar para garantir a conformidade

aws academy

Apresentação da 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



A AWS contrata órgãos de certificação externos e auditores independentes para fornecer aos clientes informações sobre as políticas, os processos e os controles estabelecidos e operados pela AWS.

Uma listagem completa dos programas de conformidade da AWS está disponível. Além disso, para saber quais serviços da AWS estão no escopo dos programas de garantia da AWS, consulte Serviços da AWS no escopo pelo programa de conformidade.

Como exemplo de uma **certificação** para a qual você pode usar serviços da AWS para cumprir seus objetivos de conformidade, considere a certificação **ISO/IEC 27001:2013**. Ela especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gerenciamento de segurança da informação. A base dessa certificação é o desenvolvimento e a implementação de um programa de segurança rigoroso, que inclui o desenvolvimento e a implementação de um Sistema de gerenciamento de segurança da informação. O Sistema de gerenciamento de segurança da informação define como a AWS gerencia permanentemente a segurança de modo holístico e abrangente.

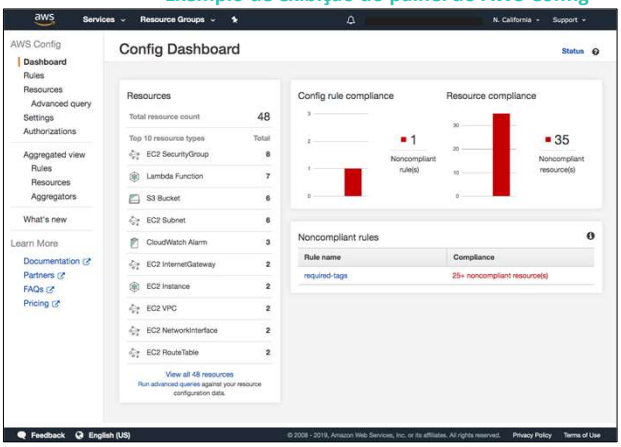
A AWS também oferece recursos de segurança e contratos legais criados para ajudar a

oferecer suporte aos clientes com regulamentações e leis comuns. Um exemplo é o regulamento da **Lei de Portabilidade e Responsabilidade de Provedores de Saúde (HIPAA) dos EUA**. Outro exemplo, o **Regulamento geral de proteção de dados (GDPR)** da União Europeia (UE) protege o direito fundamental dos titulares de dados da União Europeia à privacidade e à proteção de dados pessoais. Ele introduz requisitos robustos que elevarão e padronizarão aos padrões de proteção, segurança e conformidade dos dados. O centro do GDPR contém muitos recursos para ajudar os clientes a cumprir os requisitos de conformidade com esse regulamento.

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.**

O **AWS Config** é um serviço que permite estimar, auditar e avaliar as configurações dos recursos da AWS. O AWS Config monitora e registra continuamente as configurações de recursos da AWS e permite automatizar a avaliação das configurações registradas em relação às configurações desejadas. Com o AWS Config, você pode analisar alterações nas configurações e nos relacionamentos entre recursos da AWS, revisar históricos detalhados de configuração de recursos e determinar a conformidade geral em relação às configurações especificadas nas diretrizes internas. Dessa forma, você pode simplificar a auditoria de conformidade, a análise de segurança, o gerenciamento de mudanças e a solução de problemas operacionais.

Como você pode ver na captura de tela do painel do AWS Config mostrada aqui, o AWS Config mantém uma listagem de inventário de todos os recursos existentes na conta e, em seguida, verifica a conformidade das regras de configuração e a conformidade dos recursos. Os recursos considerados não compatíveis são sinalizados, o que alerta você sobre problemas de configuração que devem ser resolvidos na conta.

O AWS Config é um serviço regional. Para acompanhar recursos em todas as regiões, habilite-o em todas as regiões que você usar. O AWS Config oferece um recurso agregador que pode mostrar uma visualização agregada dos recursos em várias regiões e até mesmo várias contas.

AWS Artifact

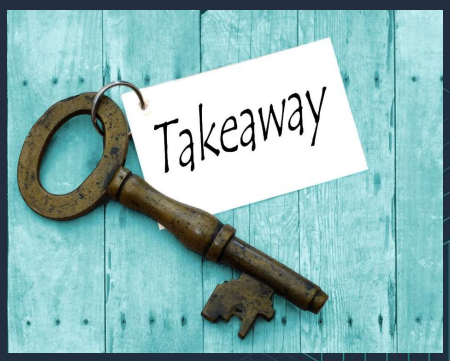
AWS Artifact

- **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).

O **AWS Artifact** disponibiliza downloads sob demanda de documentos de segurança e conformidade da AWS, como relatórios de certificações ISO da AWS, Payment Card Industry (PCI) e Service Organization Control (SOC). Você pode enviar os documentos de segurança e conformidade (também conhecidos como *artefatos de auditoria*) aos auditores ou reguladores para demonstrar a segurança e a conformidade da infraestrutura e dos serviços da AWS que você usa. Você também pode usar esses documentos como diretrizes para avaliar sua própria arquitetura de nuvem e a eficácia dos controles internos da sua empresa. O AWS Artifact fornece documentos somente sobre a AWS. Os clientes da AWS são responsáveis pelo desenvolvimento ou pela obtenção de documentos que demonstrem a segurança e a conformidade de suas empresas.

Você também pode usar o AWS Artifact para analisar, aceitar e acompanhar o status de contratos da AWS, como o Acordo de associado comercial (BAA). Normalmente, um BAA é necessário para empresas sujeitas à HIPAA para garantir que as informações de saúde protegidas (PHI) sejam protegidas de maneira adequada. Com o AWS Artifact, você pode aceitar contratos com a AWS e designar contas da AWS que podem processar legalmente informações restritas. Você pode aceitar um contrato em nome de várias contas. Para aceitar contratos para várias contas, use o AWS Organizations para criar uma organização. Para saber mais, consulte Gerenciamento de contratos no AWS Artifact.

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.

Algumas das principais lições desta seção do módulo são:

- 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 academy

Apresentação da Seção 7: Serviços e recursos de segurança adicionais

AWS Service Catalog

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

O **AWS Service Catalog** permite que as organizações criem e gerenciem catálogos de serviços de TI aprovados para uso (por exemplo, para uso dos funcionários) na AWS. Esses serviços de TI podem incluir tudo, de imagens de máquinas virtuais, servidores, software e bancos de dados a arquiteturas completas de aplicativos multicamada.

Sob a perspectiva do AWS Service Catalog, um serviço de TI pode ser considerado um produto. Um produto pode ser uma única instância de computação que executa o Amazon Linux, pode ser um aplicativo Web multicamada totalmente configurado que é executado no próprio ambiente ou pode ser qualquer outro serviço de TI útil que você crie na AWS. Isso permite que os usuários implantem rapidamente os serviços de TI de que precisam e é projetado para que os usuários implantem apenas configurações aprovadas. O AWS Service Catalog pode auxiliar seus esforços de gerenciamento centralizado de serviços de TI implantados e pode ajudar você a alcançar uma governança consistente e atender aos requisitos de conformidade.

Para saber mais, a documentação da AWS oferece mais informações sobre o AWS Service Catalog.

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.

O **Amazon Macie** é um serviço de segurança que usa machine learning para descobrir, classificar e proteger automaticamente dados confidenciais na AWS. O Amazon Macie reconhece dados confidenciais, como informações de identificação pessoal (PII) ou propriedade intelectual. Ele fornece painéis e alertas que dão visibilidade sobre como esses dados estão sendo acessados ou movidos. O Amazon Macie é um serviço totalmente gerenciado que monitora continuamente atividades de acesso a dados para detectar anomalias e gera alertas detalhados quando detecta risco de acesso não autorizado ou vazamento acidental de dados. No momento, o Amazon Macie está disponível para proteger dados armazenados no Amazon S3.

O **Amazon Inspector** é um serviço automatizado de avaliação de segurança que ajuda a melhorar a segurança e a conformidade de aplicativos implantados na AWS. O Amazon Inspector avalia automaticamente os aplicativos em busca de exposições, vulnerabilidades e discrepâncias em relação às práticas recomendadas. Depois de realizar uma avaliação, o Amazon Inspector produz uma lista detalhada de descobertas de segurança que são listadas por nível de severidade. Essas descobertas podem ser analisadas diretamente ou como parte de relatórios de avaliação detalhados que estão disponíveis por meio da API ou do console do Amazon Inspector.

O **Amazon GuardDuty** é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para

proteger contas e cargas de trabalho da AWS. Com a nuvem, a coleta e a agregação de atividades de redes e contas é simplificada, mas pode ser demorado para que as equipes de segurança analisem continuamente dados de log de eventos em busca de possíveis ameaças. O GuardDuty usa machine learning, detecção de anomalias e inteligência integrada contra ameaças para identificar e classificar possíveis ameaças. O GuardDuty analisa dezenas de bilhões de eventos em várias fontes de dados da AWS, como AWS CloudTrail, Amazon VPC Flow Logs e logs de Domain Name System (DNS).

Módulo 4: Segurança na Nuvem AWS

Conclusão do módulo

aws academy

Agora é hora de revisar o módulo e terminar com um teste de conhecimento e uma discussão sobre uma pergunta simulada de certificação.

Resumo do módulo

aws academy

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

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

Agora é hora de concluir o teste de conhecimento deste módulo.

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

Examine as opções de resposta e as exclua com base nas palavras-chave destacadas anteriormente.

Esta pergunta de exemplo vem do documento de perguntas de exemplo do exame AWS Certified Cloud Practitioner vinculado, na página principal de informações do exame AWS Certified Cloud Practitioner.

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

Segurança é um tópico extenso, e este módulo forneceu apenas uma introdução ao assunto. Os recursos a seguir fornecem mais detalhes:

- A página inicial de segurança da Nuvem AWS – fornece links para muitos recursos de segurança.
- Recursos de segurança da AWS.
- Blog de segurança da AWS.
- Os boletins de segurança notificam o cliente sobre os eventos mais recentes de segurança e privacidade com os serviços da AWS.
- A página de testes de vulnerabilidade e penetração – descreve quais tipos de testes são permitidos sem aprovação prévia, quais exigem aprovação e quais são proibidos.
- AWS Well-Architected Framework – Pilar da segurança.
- Documentação da AWS – Práticas recomendadas do IAM.

Obrigado

aws academy

Agradecemos por concluir este módulo.