Visão Geral da AWS: Modelo de responsabilidade compartilhada da AWS

Resumo

Referências Bibliográficas

- AWS Academy Cloud Foundations (Fundamentos de nuvem da AWS Academy) (PT) Instructor Guide Version 2.0.1 100-ACCLFO-20-PT-IG. 2020 Amazon Web Services, Inc. ou suas afiliadas.

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.
Vamos iniciar com a apresentação do 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).

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, que 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.

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.

O segundo serviço de Segurança apresentado é o ACF 3.0.2 **AWS IAM - Identity and Access Management.** É um componente essencial da segurança e gestão dos usuários na nuvem, 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.

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.

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 Trusted Advisor disponibiliza orientações em tempo real para ajudar você a provisionar recursos seguindo as melhores práticas da AWS.

Para saber mais sobre o AWS Trusted Advisor, consulte: http://aws.amazon.com/premiumsupport/trustedadvisor.

O **AWS Trusted Advisor** é uma ferramenta voltada para:

1. Otimização de custos
2. Performance
3. Segurança
4. Tolerância a falhas
5. Limites de serviço

O status da verificação é exibido usando codificação por cores no painel:

• Vermelho: recomendamos uma ação

• Amarelo: recomendamos uma investigação

• Verde: nenhum problema detectado

Console do Trusted Advisor: https://console.aws.amazon.com/trustedadvisor/

Finalizando os serviços de armazenamento, vem o **AWS CloudTrail,** 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.

Exercícios

1. No modelo de responsabilidade compartilhada, a AWS é responsável por fornecer o quê? (Selecione a melhor resposta.)

a) Segurança da nuvem
b) Segurança à nuvem
c) Segurança para a nuvem
d) Segurança na nuvem

2. Como um administrador de sistema incluiria uma camada adicional de segurança de login ao Console de Gerenciamento da AWS de um usuário? (Selecione a melhor resposta.)

a) Usar o Amazon Cloud Directory
b) Auditar funções do AWS Identity and Access Management (IAM)
c) Habilitar autenticação multifator
d) Habilitar o AWS CloudTrail login ao Console de Gerenciamento da AWS de um

3. Qual das seguintes opções é responsabilidade da AWS de acordo com o modelo de responsabilidade compartilhada da AWS? (Selecione a melhor resposta.)

a) Configuração de aplicações de terceiros
b) Manutenção de hardware físico
c) Acesso e dados de aplicações de segurança
d) Gerenciamento de imagens de máquina da Amazon (AMIS) personalizadas

4. Qual das seguintes opções é a melhor prática para proteger sua conta usando o AWS Identity and Access Management (IAM)? (Escolha **a melhor** alternativa.)

a) Fornecer aos usuários privilégios administrativos padrão.
b) Deixar credenciais e usuários não utilizados e desnecessários em vigor.
c) Gerenciar o acesso aos recursos da AWS
d) Evitar o uso de grupos do IAM para conceder as mesmas permissões de acesso a vários usuários.

5. Ao criar uma política do AWS Identity and Access Management (IAM), quais são os **dois** tipos de acesso que podem ser concedidos a um usuário? (Escolha **duas** alternativas.)

a) Acesso institucional
b) Acesso autorizado
c) Acesso programático
d) Acesso ao Console de Gerenciamento da AWS
e) Acesso raiz administrativo

6. No modelo de responsabilidade compartilhada, quais são as duas das opções a seguir que são exemplos de “segurança na nuvem”? (Escolha **duas** alternativas.)

a) Conformidade com padrões e regulamentos de segurança de computação
b) Segurança física das instalações em que os serviços operam
c) Configurações do grupo de segurança
d) Criptografia de dados ociosos e dados em trânsito
e) Proteção da infraestrutura global

descomplica

impulsotec

Gabarito

1. **A**

   A letra a é a alternativa correta, pois, no modelo de responsabilidade compartilhada, a AWS é responsável por fornecer a segurança da nuvem

2. **C**.

   A letra c é a alternativa correta, pois, para incluir uma camada adicional de segurança do usuário, habilite a autenticação multifator

3. **B**

   A letra b é a alternativa correta, pois A manutenção de hardware físico é responsabilidade da AWS sob o modelo de responsabilidade compartilhada

4. **C**

   A letra c é a alternativa correta, pois gerenciar o acesso aos recursos da AWS é melhor prática para proteger contas com o AWS IAM.

5. **C e D**

   As letras c e d são as alternativas corretas, pois ao criar uma política de IAM, um usuário pode receber acesso ao Console de Gerenciamento da AWS e acesso programático

6. **C e D**

   As letras c e d são as alternativas corretas, pois “Criptografia de dados ociosos e de dados em trânsito” e “Configurações de grupos de segurança” são exemplos de segurança na nuvem