

Questões

quarta-feira, 30 de agosto de 2023

15:37

2

A possibilidade de dimensionar horizontalmente as instâncias do Amazon EC2 sob demanda é um exemplo de qual conceito na proposta de valor da AWS Cloud?

- A** Economia de dimensionamento
- B** Elasticidade
- C** Alta disponibilidade
- D** Agilidade

Resposta: Elasticidade

Qual despesa on-premises será reduzida se a empresa migrar o aplicativo para o Amazon EC2?

- A** Custos do hardware do servidor
- B** Custos do armazenamento no Amazon EBS
- C** Custos de backup do armazenamento
- D** Custos da transferência de dados para fora da Internet

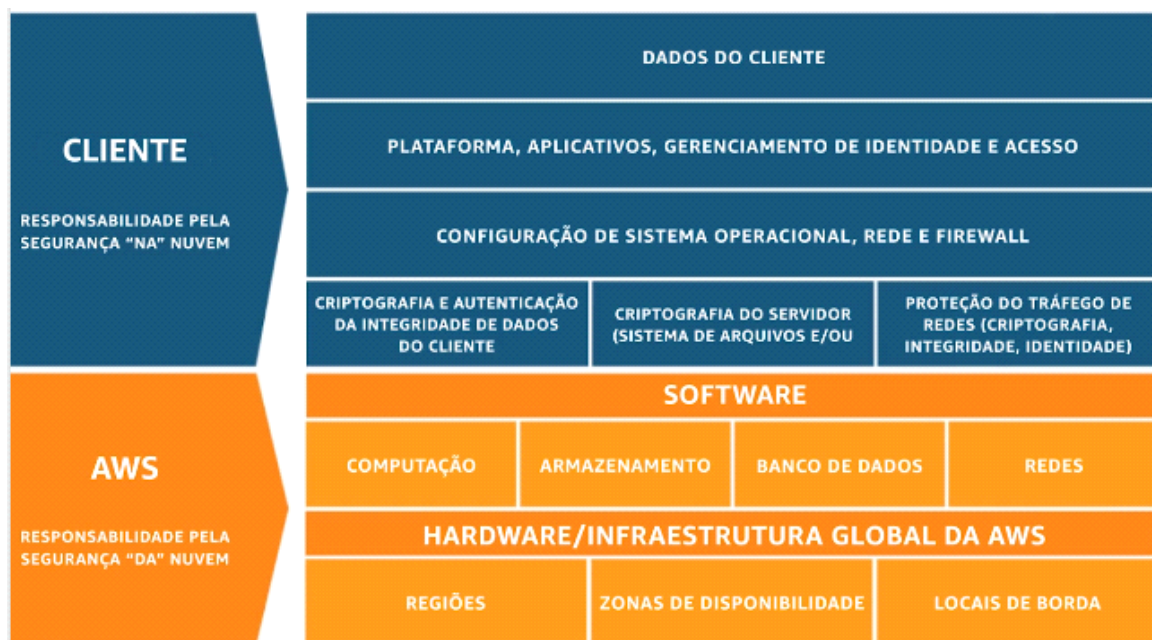
Resposta: Custos de hardware do servidor

Q

Qual das opções representa um princípio de projeto de arquitetura da AWS Cloud?

- A Implementar pontos únicos de falha
- B Implementar acoplamento fraco
- C Implementar projeto monolítico
- D Implementar scaling vertical

Resposta: implementar acoplamento fraco



Modelo de responsabilidade compartilhada AWS

Q

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

- A** Aplicação de patches na infraestrutura subjacente
- B** Segurança física
- C** Aplicação de patches nas instâncias do Amazon EC2
- D** Aplicação de patches na infraestrutura de rede

Resposta: Aplicação de patches nas instâncias do Amazon EC2

Q

Qual é o serviço que auxilia na auditoria de risco com o monitoramento e o registro contínuos da atividade da conta, incluindo as ações dos usuários no AWS Management Console e no SDK da AWS?

- A** Amazon CloudWatch
- B** AWS CloudTrail
- C** AWS Config
- D** AWS Health

Resposta: AWS CloudTrail

Diferença entre AWS CloudWatch, AWS CloudTrail, AWS Cloud config e AWS CloudHearth

- **AWS CloudWatch** - Serviço de monitoramento que permite monitorar dados gerados por recursos e visualizá-los como estatísticas nos painéis do CloudWatch, apesar de monitorar continuamente, ele não ativa de fato nenhum tipo de auditoria de risco.
 - Pode fornecer informações sobre se você tem uma instância sobrecarregada do EC2
 - Números altos de solicitações atingindo um Elastic Load Balancer.
 - Não permite que você audite chamadas de API feitas recentemente em sua conta AWS.

- **AWS CloudTrail**
 - Permite que você audite chamadas de API feitas recentemente em sua conta AWS
 - Registro em log
 - Qualquer atividade feita no console ou usando os SDKs (Assumir um perfil ou excluir uma instância do EC2)
- **AWS CloudConfig** é um serviço para avaliar, analisar e auditar as configurações dos recursos da AWS.
 - Auditar e examinar as configurações de seus recursos da AWS
 - Monitora e registra continuamente suas configurações de recursos da AWS
 - Permite automatizar as avaliações das configurações registradas em relação as configurações desejadas
 - Permite auditar, monitora e registra continuamente a configuração de recursos
 - Registra apenas as mudanças de configurações de recursos
- **AWS Health** fornece visibilidade contínua para o desempenho de seu recurso da AWS
 - Disponibilidade dos serviços da AWS que você usa
 - Não registra nenhuma atividade da conta nem permite realizar uma auditoria de risco com base nessa atividade da conta.

Acess Management Capabilities

A partir da criação da conta na AWS o tipo de identidade é chamada de usuário-raiz da conta AWS.

- Pode-se usar as políticas de IAM para controlar ao que os usuários do AWS tem acesso
 - Quais chamadas de API o usuário tem permissão de fazer, isso inclui chamadas de API para acessar recursos como buckets do Amazon S3.
- **Usuário Raiz**
 - Tem acesso irrestrito e completo a todos os recursos em uma conta AWS
 - Não se deve usar esse usuário para realizar tarefas diárias
- Use a **MFA** (Autenticação com multifator) para o usuário raiz
- Alternar as chaves de acesso e senha para o usuário raiz
- Não usar o usuário-raiz para tarefas diárias
- Criar outros usuários do IAM para fazer tarefas diárias

- **Recursos do IAM:**

- Usuários
- Grupos
- Perfis
- Políticas
 - Políticas gerenciadas - AWS cria e gerencia políticas gerenciadas
 - Não gerenciadas - Clientes criam e gerenciam políticas regulares do IAM

Os perfis do IAM são identidades usadas que dão credenciais temporárias

Qual destes itens pode limitar o acesso de buckets do Amazon Simple Storage Service (Amazon S3) a determinados usuários?	
A	Pares de chaves públicas e privadas
B	Amazon Inspector
C	Políticas do AWS Identity and Access Management (IAM)
D	Grupos de segurança

Resposta: Políticas do AWS identity and Access Management(IAM)

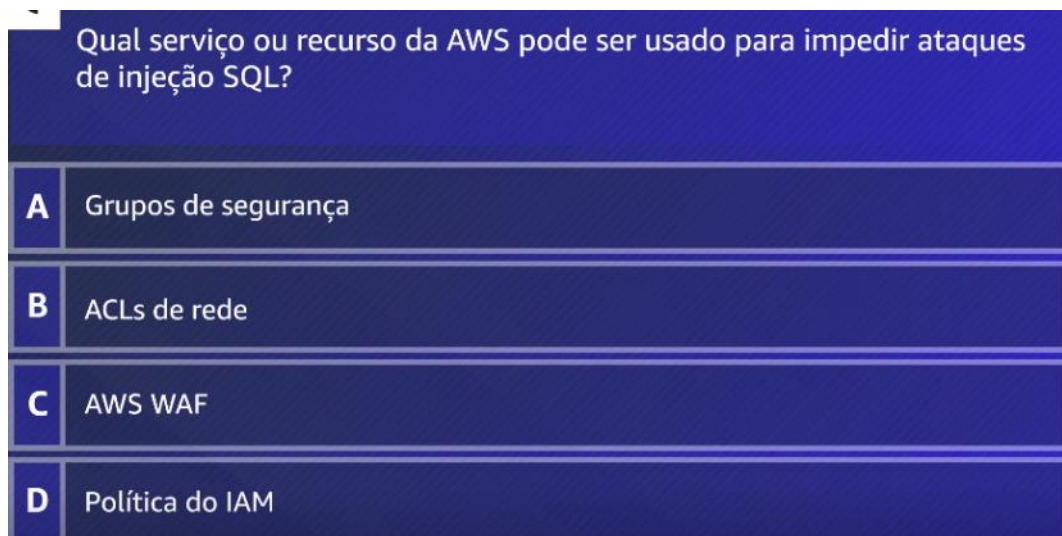
- **Pares de chaves públicas e privadas**
 - Não se usa para acessar uma bucket S3
- **A bucket S3** é controlado por meio de política do bucket S3 e das políticas do IAM aplicadas às identidades que tentam acessar a S3.
- **Amazon Inspector** é um serviço que executa avaliações de segurança nas instâncias do Amazon EC2.
- **Grupos de Segurança** são firewalls no **nível da instância** para controlar acesso às instâncias do Amazon EC2 não aos buckets o Amazon S3.
 - Não podem impedir ataques SQL
 - Permitem tráfegos com base em Porta, Protocolo e origem ou destino.
 - Portanto não inspecionam um pacote HTTP

Resources for security support

Identifique recursos para o suporte de segurança

- **Segurança de rede**
 - Grupos de segurança

- Listas de controle de acesso à rede (ACLs de rede)
- AWS Web Application Firewall
- AWS WAF
- **AWS Trusted Advisor**
- **Amazon Inspector**
- **AWS Marketplace** - Encontrar serviços de terceiros para utilizar.
- **AWS Knowledge center** é um local para encontrar respostas as suas perguntas
- **Security Center** é outro local para obter informações relacionadas a segurança na AWS
- **AWS Security Forum** para encontrar informações de segurança da AWS



Resposta: AWS WAF

- **AWS WAF ou Web Application Firewall** é um firewall que pode filtrar tráfego com base em qualquer parte da solicitação como
 - ☐ endereços IP
 - ☐ cabeçalhos HTTP
 - ☐ Corpo HTTP
 - ☐ Cadeias de Caracteres URI
- **ACLs de Rede** podem permitir ou negar tráfegos com base em
- **ACLs de rede** estão em nível de sub-rede
 - ☐ Tipo do tráfego
 - ☐ Porta
 - ☐ Protocolo
 - ☐ Origem ou destino