examundo

Simulado AWS Solutions Architect Associate em português

69 questões com respostas. Os guias e as traduções foram feitos e revisados por software. Ainda não foram revisados por nenhuma pessoa.

Atualizado em 25 de novembro de 2026 · examundo.tech/pt/aws-solutions-architect-associate/

Arquiteturas de alto desempenho

1. Um cluster de HPC que executa cargas MPI fortemente acopladas em instâncias c5n.18xlarge precisa contornar o kernel do sistema operacional na comunicação entre nós para obter a menor latência possível em escala. Qual recurso de rede deve ser anexado às instâncias?

An HPC cluster running tightly coupled MPI workloads across c5n.18xlarge instances needs to bypass the operating system kernel for inter-node communication to achieve the lowest possible latency at scale. Which networking feature should be attached to the instances?

A. Rede aprimorada com o Elastic Network Adapter (ENA)

B. AWS Global Accelerator com endereços IP estáticos anycast

C. Uma segunda Elastic Network Interface (ENI) para separar o tráfego

D. Elastic Fabric Adapter (EFA)

---

2. Uma aplicação faz milhões de leituras por segundo em uma tabela do DynamoDB e precisa de tempos de resposta na casa dos microssegundos, sem alterar o modelo de dados da aplicação. Qual solução atende MELHOR a isso?

An application performs millions of reads per second against a DynamoDB table and requires microsecond-level response times without modifying the application's data model. Which solution BEST achieves this?

A. DynamoDB Global Tables

B. Amazon DynamoDB Accelerator (DAX)

C. Amazon ElastiCache for Redis na frente do DynamoDB

D. DynamoDB Auto Scaling com mais RCUs provisionadas

---

3. Uma empresa de mídia processa trabalhos curtos de transcodificação de vídeo, que duram só alguns minutos e ocorrem em intervalos imprevisíveis ao longo do dia. Qual opção de computação é a MAIS econômica e exige MENOS gerenciamento de infraestrutura?

A media company processes short video transcoding jobs that run for only a few minutes at unpredictable intervals throughout the day. Which compute option is MOST cost-effective and requires the LEAST infrastructure management?

A. Um grupo do Amazon EC2 Auto Scaling com no mínimo uma instância sob demanda (On-Demand)

B. Amazon Lightsail com uma instância de tamanho fixo

C. AWS Lambda

D. Instâncias reservadas do EC2 em execução contínua

---

4. Uma carga de data warehouse exige um único volume EBS que entregue 200.000 IOPS e 3.000 MB/s de taxa de transferência, com latência consistente abaixo de um milissegundo, anexado a um tipo de instância EC2 compatível com io2. Qual tipo de volume atende a esse requisito?

A data warehouse workload requires a single EBS volume delivering 200,000 IOPS and 3,000 MB/s throughput with consistent sub-millisecond latency, attached to an io2-eligible EC2 instance type. Which volume type can meet this requirement?

A. io2 Block Express

B. gp3, aumentando o IOPS e a taxa de transferência provisionados acima da base

C. st1 com vários volumes em striping (RAID 0)

D. io2 padrão (sem Block Express)

---

5. Usuários da Ásia, da Europa e da América do Sul enviam arquivos de mídia grandes (2 a 10 GB) direto para um único bucket do S3 em us-east-1, e os tempos de upload são inconsistentes e lentos. Qual solução melhora MAIS o desempenho de upload para todas as regiões?

Users across Asia, Europe, and South America upload large media files (2-10 GB) directly to a single S3 bucket located in us-east-1, and upload times are inconsistent and slow. Which solution BEST improves upload performance for all regions?

A. Ativar apenas o upload multipart, sem outras mudanças

B. Ativar o S3 Transfer Acceleration no bucket

C. Replicar o bucket em todas as regiões com o S3 Cross-Region Replication

D. Criar uma distribuição do CloudFront na frente do bucket

---

6. Um arquiteto de soluções precisa escalar o tráfego de leitura de um banco de dados compatível com MySQL e exige atraso de réplica (replica lag) tipicamente abaixo de 100 milissegundos, com suporte a até 15 réplicas de leitura que compartilhem o mesmo armazenamento da instância primária. Qual solução atende a esses requisitos?

A solutions architect must scale read traffic for a MySQL-compatible database and needs replica lag typically under 100 milliseconds, along with support for up to 15 read replicas that share the same underlying storage as the primary instance. Which solution meets these requirements?

A. Amazon Aurora MySQL com réplicas do Aurora

B. Amazon DynamoDB Accelerator (DAX)

C. Amazon RDS for MySQL com réplicas de leitura

D. Implantação Multi-AZ do Amazon RDS for MySQL

---

7. Um arquiteto de soluções projeta o armazenamento de um banco de dados relacional crítico no Amazon EC2, que exige até 200.000 IOPS e latência consistente abaixo de um milissegundo. Qual tipo de volume EBS o arquiteto deve escolher?

A solutions architect is designing storage for a mission-critical relational database on Amazon EC2 that requires up to 200,000 IOPS and sub-millisecond, consistent latency. Which EBS volume type should the architect select?

A. SSD de uso geral (gp3)

B. HDD frio (sc1)

C. SSD de IOPS provisionado (io2 Block Express)

D. HDD otimizado para taxa de transferência (st1)

---

8. Uma empresa global de mídia quer reduzir a latência de usuários que assistem a vídeos em streaming, mantendo cópias do conteúdo em locais fisicamente mais próximos dos usuários finais. Qual serviço da AWS deve ser usado?

A global media company wants to reduce latency for users streaming video content by caching copies of the content at locations physically closer to end users. Which AWS service should be used?

A. Amazon ElastiCache

B. AWS Direct Connect

C. Amazon Route 53

D. Amazon CloudFront

---

9. Um site global de comércio eletrônico usa o CloudFront com pontos de presença em vários continentes, e o servidor de origem sofre alta carga por falhas repetidas de cache (cache misses) nos caches regionais para os mesmos objetos. Qual recurso do CloudFront o arquiteto de soluções deve ativar para reduzir a carga na origem?

A global e-commerce site uses CloudFront with edge locations on multiple continents, and the origin server is experiencing high load from repeated cache misses across regional edge caches for the same objects. Which CloudFront feature should the solutions architect enable to reduce origin load?

A. URLs assinadas (signed URLs)
B. Criptografia em nível de campo (field-level encryption)
C. Gatilhos de requisição de origem do Lambda@Edge
D. Origin Shield

---

10. Um site global servido pelo Amazon CloudFront sofre alta carga nos servidores de origem porque muitos pontos de presença buscam, cada um por conta própria, os mesmos objetos, raramente presentes no cache, quando ocorre um cache miss. Qual recurso é o MELHOR para reduzir essa carga na origem sem alterar a estratégia de TTL do cache?

A global website served through Amazon CloudFront experiences high load on its origin servers because many edge locations independently fetch the same rarely-cached objects from the origin during cache misses. Which feature BEST reduces this origin load without changing the caching TTL strategy?

A. Aumentar o TTL do cache de todos os objetos
B. Aumentar a capacidade de computação do servidor de origem
C. Ativar o CloudFront Origin Shield
D. Implantar o Lambda@Edge para servir conteúdo estático

---

11. Uma aplicação grava em um bucket do Amazon S3 a uma taxa constante de 12.000 requisições PUT por segundo, com todas as chaves de objeto começando com o mesmo prefixo. O desempenho dos uploads está caindo. Qual é a solução MAIS eficaz?

An application writes to an Amazon S3 bucket at a sustained rate of 12,000 PUT requests per second, with all object keys beginning with the same prefix. Upload performance is degrading. What is the MOST effective solution?

A. Ativar o S3 Versioning no bucket
B. Mudar a classe de armazenamento para S3 Standard-IA
C. Distribuir os objetos em vários prefixos de chave
D. Ativar o S3 Transfer Acceleration no bucket

---

12. Uma aplicação em cluster, executada em várias instâncias EC2 na mesma zona de disponibilidade, exige armazenamento em blocos compartilhado e de baixa latência, com acesso simultâneo de leitura e gravação de até 16 instâncias. Qual solução atende a esse requisito?

A clustered application running on multiple EC2 instances in the same Availability Zone requires shared, low-latency block storage with concurrent read/write access from up to 16 instances. Which solution meets this requirement?

A. Amazon S3 com Transfer Acceleration
B. Amazon EBS io2 com Multi-Attach
C. Amazon EFS
D. Amazon EBS gp3 com snapshots

---

13. Uma aplicação de HPC fortemente acoplada exige a menor latência de rede possível e a maior taxa de transferência entre instâncias EC2 em uma única zona de disponibilidade. Qual estratégia de posicionamento (placement) do EC2 o arquiteto deve usar?

A tightly coupled HPC application requires the lowest possible network latency and highest throughput between EC2 instances within a single Availability Zone. Which EC2 placement strategy should the architect use?

A. Grupo de posicionamento em cluster (cluster placement group)
B. Grupo de posicionamento distribuído (spread placement group)
C. Posicionamento padrão (sem grupo)
D. Grupo de posicionamento por partição (partition placement group)

---

14. Um arquiteto de soluções quer reduzir a carga de leitura de um banco de dados relacional, guardando em memória os resultados de consultas acessados com frequência. Qual serviço da AWS foi feito para essa finalidade?

A solutions architect wants to reduce read load on a relational database by caching frequently accessed query results in memory. Which AWS service is designed for this purpose?

A. Amazon DynamoDB Accelerator (DAX)
B. AWS Storage Gateway
C. Amazon ElastiCache
D. Amazon CloudFront

---

15. Uma empresa de jogos precisa de um cache simples em memória para guardar dados de sessão e quer aproveitar o processamento multithread para maximizar a taxa de transferência em um único nó de cache grande. Qual mecanismo de cache o arquiteto de soluções deve escolher?

A gaming company needs a simple in-memory cache to store session data and wants to take advantage of multi-threaded processing to maximize throughput on a single large cache node. Which caching engine should the solutions architect select?

A. Amazon ElastiCache for Redis
B. Amazon DynamoDB Accelerator (DAX)
C. Amazon ElastiCache for Memcached
D. Amazon RDS Proxy

---

16. Uma empresa de jogos executa um cache de estado de sessão no ElastiCache e quer maximizar a vazão por nó, usando todos os núcleos de CPU da instância. Os dados não exigem persistência, replicação nem estruturas de dados complexas. Qual mecanismo do ElastiCache atende MELHOR a esse requisito?

A gaming company runs an ElastiCache session-state cache and wants to maximize throughput per node by fully utilizing all CPU cores on the underlying instance. The data does not require persistence, replication, or complex data structures. Which ElastiCache engine BEST meets this requirement?

A. Memcached
B. Redis com modo cluster desativado
C. Redis com modo cluster ativado
D. Redis com Multi-AZ e failover automático

---

17. Uma empresa hospeda ativos estáticos de um site em um bucket do S3 em us-east-1 e atende usuários na América do Norte, na Europa e na Ásia. Usuários da Ásia relatam carregamento lento das páginas. Qual solução traz a MAIOR melhoria de desempenho com o MENOR esforço operacional?

A company hosts static website assets in an S3 bucket in us-east-1 and serves users across North America, Europe, and Asia. Users in Asia report slow page load times. Which solution provides the MOST performance improvement with the LEAST operational overhead?

A. Implantar uma distribuição do Amazon CloudFront com o bucket do S3 como origem

B. Criar replicação entre regiões do S3 para buckets em cada região

C. Aumentar o tamanho da instância EC2 que hospeda o servidor web

D. Ativar o S3 Transfer Acceleration no bucket

Arquiteturas seguras

18. Uma organização quer permitir que desenvolvedores criem funções (IAM roles) e políticas do IAM para os próprios projetos, mas precisa garantir que nenhum desenvolvedor consiga conceder a uma função permissões acima de um máximo predefinido, não importa a política que anexe. Qual recurso do IAM o arquiteto de soluções deve implementar?

An organization wants to allow developers to create IAM roles and policies for their own projects, but must guarantee that no developer can grant a role permissions broader than a predefined maximum, regardless of the policy they attach. Which IAM feature should the solutions architect implement?

A. Uma política de grupo do IAM mais restritiva do que qualquer política que os desenvolvedores possam anexar

B. Uma política de controle de serviço (SCP) anexada à unidade organizacional dos desenvolvedores

C. Um limite de permissões anexado a cada função do IAM que os desenvolvedores criarem

D. Uma política baseada em recurso em cada recurso que as funções vão acessar

19. Um arquiteto de soluções projeta uma aplicação em instâncias EC2 que precisa ler objetos de um bucket do S3. Qual abordagem oferece a forma MAIS segura de conceder esse acesso?

A solutions architect is designing an application running on EC2 instances that needs to read objects from an S3 bucket. Which approach provides the MOST secure method for granting this access?

A. Incorporar as credenciais do usuário raiz (root) da conta no arquivo de configuração da aplicação

B. Criar um usuário do IAM com acesso ao S3 e deixar as credenciais fixas no código da aplicação

C. Anexar ao perfil de instância do EC2 uma função do IAM com uma política que conceda s3:GetObject

D. Guardar as chaves de acesso de um usuário do IAM nas variáveis de ambiente da instância EC2

20. Uma empresa de comércio eletrônico na AWS quer o acompanhamento proativo da equipe de resposta a DDoS da AWS (DRT) e proteção de custos contra as cobranças de escala geradas durante um ataque DDoS em larga escala. Qual nível de serviço o arquiteto deve ativar?

An e-commerce company running on AWS wants proactive engagement from the AWS DDoS Response Team (DRT) and cost protection against scaling charges incurred during a large-scale DDoS attack. Which service tier should the architect enable?

A. Amazon GuardDuty com a proteção do S3 ativada

B. AWS Shield Standard, incluído automaticamente para todos os clientes

C. AWS Shield Advanced

D. AWS WAF apenas com regras baseadas em taxa

21. Um arquiteto de soluções precisa garantir que os dados dos volumes do Amazon EBS anexados a instâncias EC2 sejam criptografados em repouso, inclusive todos os snapshots criados a partir deles, com o mínimo de esforço operacional. Qual abordagem o arquiteto deve adotar?

A solutions architect must ensure that data stored on Amazon EBS volumes attached to EC2 instances is encrypted at rest, including all snapshots created from those volumes, with minimal operational overhead. Which approach should the architect take?

A. Ativar a criptografia padrão do S3 no bucket em que os snapshots são armazenados

B. Aplicar uma política do IAM que negue a criação de volumes não criptografados, sem ativar a criptografia no nível da conta

C. Criptografar manualmente cada snapshot depois de criado, com um utilitário de criptografia de disco de terceiros

D. Ativar a criptografia do EBS por padrão para a conta e a região, de modo que os novos volumes e seus snapshots sejam criptografados automaticamente com o AWS KMS

---

22. Uma empresa de serviços financeiros guarda documentos sensíveis no Amazon S3 e precisa auditar cada uso da chave de criptografia, inclusive qual principal descriptografou determinado objeto e quando. Qual opção de criptografia atende a esse requisito?

A financial services company stores sensitive documents in Amazon S3 and must be able to audit every use of the encryption key, including which principal decrypted a given object and when. Which encryption option satisfies this requirement?

A. Criptografia no cliente (client-side) com uma chave guardada localmente

B. SSE-C com uma chave fornecida em cada requisição

C. SSE-S3 com chaves gerenciadas pelo Amazon S3

D. SSE-KMS com uma CMK gerenciada pelo cliente

---

23. Uma empresa conecta seu data center local a uma VPC por meio do AWS Direct Connect. Os servidores locais precisam acessar buckets do Amazon S3 de forma privada, sem passar pela internet pública e sem usar um NAT gateway ou proxy. Qual solução atende a esse requisito?

A company connects its on-premises data center to a VPC using AWS Direct Connect. On-premises servers must reach Amazon S3 buckets privately, without traversing the public internet and without using a NAT gateway or proxy. Which solution meets this requirement?

A. Ativar o S3 Transfer Acceleration nos buckets de destino

B. Anexar um internet gateway à VPC e restringir o acesso por uma condição na bucket policy sobre a VIF do Direct Connect

C. Criar um endpoint de VPC de gateway para o S3 e atualizar as tabelas de rotas da VPC

D. Criar um endpoint de VPC de interface para o S3 e atualizar o DNS local para resolver para os IPs privados do endpoint

---

24. Uma bucket policy restringe o acesso com uma condição aws:SourceIp limitada ao bloco CIDR privado de uma VPC corporativa, 10.20.0.0/16. As instâncias EC2 dessa VPC acessam o S3 pelo caminho da internet pública, por meio de um NAT gateway. As requisições são negadas de forma inesperada. Qual é a causa raiz?

A bucket policy restricts access using a condition on aws:SourceIp limited to a corporate VPC's private CIDR block, 10.20.0.0/16. EC2 instances in that VPC access S3 over the public internet path through a NAT gateway. Requests are unexpectedly denied. What is the root cause?

A. O bloco CIDR privado precisa ser adicionado à configuração de CORS do bucket

B. O NAT gateway reescreve o IP de origem para o seu próprio Elastic IP público, que fica fora do CIDR permitido

C. As bucket policies do S3 não conseguem avaliar aws:SourceIp para nenhum tráfego originado em uma VPC

D. O aws:SourceIp só avalia endereços IPv6 quando as instâncias usam um NAT gateway

---

25. Qual serviço da AWS foi criado especificamente para oferecer proteção gerenciada contra ataques de negação de serviço distribuída (DDoS)?

Which AWS service is purpose-built to provide managed protection against Distributed Denial of Service (DDoS) attacks?

A. AWS Firewall Manager

B. AWS WAF

C. Amazon GuardDuty

D. AWS Shield

---

26. Uma empresa precisa criptografar objetos no Amazon S3 e manter uma trilha de auditoria detalhada de cada uso da chave de criptografia, inclusive quem a acessou e quando. Qual opção de criptografia atende a esse requisito?

A company must encrypt objects in Amazon S3 and maintain a detailed audit trail of every use of the encryption key, including who accessed it and when. Which encryption option meets this requirement?

A. Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

B. Criptografia no cliente com uma chave AES-256 gerada localmente e guardada no código da aplicação

C. Criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS), usando o AWS CloudTrail para registrar o uso da chave

D. Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), enviadas em cada requisição

---

27. Um arquiteto de soluções precisa criar, gerenciar e controlar de forma centralizada o acesso às chaves criptográficas usadas para criptografar objetos armazenados no Amazon S3. Qual serviço da AWS deve ser usado?

A solutions architect needs to centrally create, manage, and control access to the cryptographic keys used to encrypt objects stored in Amazon S3. Which AWS service should be used?

A. AWS Systems Manager Parameter Store

B. AWS Secrets Manager

C. AWS Key Management Service (KMS)

D. AWS Certificate Manager (ACM)

---

28. Um arquiteto de soluções escreve uma política do IAM para um grupo de desenvolvedores que precisam ler e gravar objetos apenas no prefixo 'dev-uploads' de um único bucket do S3 e não podem acessar nenhum outro bucket da conta. Qual desenho de política segue o princípio do privilégio mínimo?

A solutions architect is writing an IAM policy for a group of developers who must be able to read and write objects only within the 'dev-uploads' prefix of a single S3 bucket, and must not access any other bucket in the account. Which policy design follows the principle of least privilege?

A. Conceder s3:GetObject e s3:PutObject em Resource "*" e contar com a bucket policy para restringir o acesso

B. Anexar a política gerenciada AmazonS3FullAccess e confiar na disciplina dos desenvolvedores

C. Conceder ações s3:* com um elemento Resource restrito a arn:aws:s3:::company-bucket/dev-uploads/*

D. Conceder s3:GetObject e s3:PutObject com um elemento Resource restrito a arn:aws:s3:::company-bucket/dev-uploads/*

---

29. Um usuário tem uma política do IAM baseada em identidade que permite s3:GetObject em todos os recursos. Ele também é membro de um grupo cuja política nega de forma explícita s3:GetObject em um bucket específico. Quando o usuário tenta obter um objeto desse bucket, qual é o resultado?

A user has an IAM identity-based policy that allows s3:GetObject on all resources. The user is also a member of a group whose policy explicitly denies s3:GetObject on a specific bucket. When the user attempts to retrieve an object from that bucket, what is the result?

A. O acesso é permitido, pois a política de permissão do usuário tem precedência sobre as políticas de grupo

B. O acesso é negado, pois uma negação explícita em qualquer política aplicável sempre prevalece sobre uma permissão

C. O acesso é permitido, pois o IAM avalia só a política anexada mais recentemente

D. O acesso só é negado se a instrução de negação estiver anexada direto ao usuário, e não a um grupo

---

30. Uma função do IAM (IAM role) na Conta B (333333333333) tem uma política baseada em identidade que concede kms:Decrypt com Resource definido como "*". A função tenta descriptografar um objeto do S3 criptografado com uma chave KMS gerenciada pelo cliente, de propriedade da Conta A (222222222222), e recebe um erro AccessDenied. Qual é a causa MAIS provável?

An IAM role in Account B (333333333333) has an identity-based policy granting kms:Decrypt with Resource set to "*". The role attempts to decrypt an S3 object encrypted with a customer-managed KMS key owned by Account A (222222222222) and receives an AccessDenied error. What is the MOST likely cause?

A. A política de chave da CMK na Conta A não inclui uma instrução que conceda kms:Decrypt a principais da Conta B

B. O elemento Resource da política do IAM precisa referenciar o ARN específico da chave, e não um curinga, em chamadas entre contas

C. A bucket policy do S3 na Conta A precisa permitir, em separado, a ação kms:Decrypt para a Conta B

D. A função precisa de uma concessão (grant) do KMS, e não de uma política do IAM baseada em identidade, para fazer operações de descriptografia

---

31. Um arquiteto de soluções explica como o AWS KMS criptografa objetos grandes de forma eficiente. Qual afirmação descreve MELHOR o processo de criptografia de envelope (envelope encryption) usado pelo KMS?

A solutions architect is explaining how AWS KMS encrypts large objects efficiently. Which statement BEST describes the envelope encryption process used by KMS?

A. O KMS guarda o objeto em texto simples direto dentro da chave mestra do cliente

B. O KMS criptografa o objeto inteiro direto com a chave mestra do cliente, sem chave intermediária

C. O KMS exige que a aplicação gere e gerencie manualmente a própria chave AES, sem chamar a API do KMS

D. O KMS gera uma chave de dados que criptografa o objeto localmente, e essa chave, já criptografada, é guardada junto com o texto cifrado

---

32. Uma equipe guarda a senha de um banco de dados do Amazon RDS e quer que ela seja trocada automaticamente (rotação) a cada 30 dias, com uma função de rotação do Lambda já pronta, sem escrever lógica de rotação personalizada. Qual serviço atende MELHOR a esse requisito?

A team stores an Amazon RDS database password and wants it automatically rotated every 30 days using a built-in Lambda rotation function, without writing custom rotation logic. Which service BEST satisfies this requirement?

A. AWS KMS com a rotação anual automática de chaves ativada

B. AWS Systems Manager Parameter Store com parâmetros SecureString

C. AWS Secrets Manager com suporte nativo de rotação para o RDS

D. Tokens de autenticação de banco de dados do IAM

---

33. Durante uma investigação de segurança, um arquiteto precisa descobrir quais endereços IP de origem enviaram tráfego à interface de rede elástica (ENI) de uma instância EC2 específica e se esse tráfego foi aceito ou rejeitado pelo security group. Qual serviço da AWS fornece essa informação?

During a security investigation, an architect needs to determine which source IP addresses sent traffic to a specific EC2 instance's elastic network interface and whether that traffic was accepted or rejected by the security group. Which AWS service provides this information?

A. AWS CloudTrail

B. VPC Flow Logs

C. Amazon Inspector

D. AWS Config

---

34. Uma equipe de aplicação precisa restringir o tráfego de saída de uma sub-rede de aplicação para que as instâncias só alcancem uma lista aprovada de nomes de domínio externos (por exemplo, api.partner.com), independentemente do endereço IP de destino, que muda com frequência. Qual controle impõe esse requisito?

An application team must restrict outbound traffic from an application subnet so instances can only reach a specific approved list of external domain names (e.g., api.partner.com), regardless of the destination IP address, which changes frequently. Which control enforces this requirement?

A. AWS Network Firewall com um grupo de regras com estado baseado em domínio, que permita os FQDNs aprovados

B. Uma regra de saída de NACL que permita HTTPS para os endereços IP atuais dos domínios aprovados

C. Uma política de endpoint de gateway do S3 restrita aos domínios aprovados do parceiro

D. Uma regra de saída de security group com os intervalos CIDR de destino dos domínios aprovados

---

35. Um administrador de banco de dados descobre que uma instância de produção do RDS for MySQL foi criada sem a criptografia em repouso ativada. Agora a conformidade exige que todos os dados em repouso sejam criptografados com uma chave KMS gerenciada pelo cliente, com o mínimo de indisponibilidade. Qual é a sequência correta de ações?

A database administrator discovers that an existing production RDS for MySQL instance was launched without encryption at rest enabled. Compliance now requires all data at rest to be encrypted using a customer managed KMS key, with minimal downtime. What is the correct sequence of actions?

A. Criar uma réplica de leitura com criptografia ativada e promovê-la para substituir a instância primária

B. Fazer um snapshot da instância não criptografada, copiar o snapshot com a criptografia ativada e restaurar uma nova instância a partir da cópia criptografada

C. Modificar a instância do RDS existente, ativar a opção 'Criptografia em repouso' e reiniciá-la para aplicar a mudança

D. Ativar a criptografia direto na instância em execução, pelo comando modify-db-instance da AWS CLI

Arquiteturas com custo otimizado

36. Um arquiteto de soluções precisa executar um trabalho de processamento em lote tolerante a falhas, que pode ser interrompido a qualquer momento, em troca do maior desconto possível em relação ao preço sob demanda (On-Demand). Qual opção de compra do EC2 é a MAIS adequada?

A solutions architect needs to run a fault-tolerant batch processing job that can be interrupted at any time in exchange for the deepest possible discount off On-Demand pricing. Which EC2 purchasing option is MOST appropriate?

A. Instâncias reservadas padrão (Standard Reserved Instances)

B. Instâncias Spot

C. Instâncias sob demanda (On-Demand)

D. Hosts dedicados (Dedicated Hosts)

---

37. Uma empresa executa uma carga de banco de dados de forma contínua, 24 horas por dia, pelos próximos três anos e quer minimizar o custo de computação com um compromisso firme de capacidade. Qual opção de compra dá o maior desconto para essa carga de estado estável?

A company runs a database workload continuously, 24 hours a day, for the next three years and wants to minimize compute cost with a firm capacity commitment. Which purchasing option provides the largest discount for this steady-state workload?

A. Instâncias reservadas padrão (Standard Reserved Instances) com prazo de 3 anos

B. Instâncias reservadas conversíveis (Convertible Reserved Instances) com prazo de 1 ano

C. Instâncias Spot

D. Instâncias sob demanda (On-Demand)

---

38. Uma empresa serve arquivos de vídeo grandes direto do Amazon S3 para usuários do mundo todo, com altas cobranças de transferência de dados de saída (OUT). Qual mudança MAIS reduz esses custos e ainda melhora o desempenho?

A company serves large video files directly from Amazon S3 to users worldwide, incurring high data transfer OUT charges. Which change MOST reduces these costs while also improving performance?

A. Implantar o Amazon CloudFront na frente do bucket do S3, usando um Origin Access Control

B. Ativar o S3 Transfer Acceleration no bucket

C. Mover os arquivos de vídeo para o S3 One Zone-Infrequent Access

D. Replicar o bucket em todas as regiões da AWS com o Cross-Region Replication

---

39. Um banco de dados de produção exige 16.000 IOPS e 500 MB/s de taxa de transferência sustentados em um volume de 500 GB. Qual tipo de volume EBS atende a esse requisito pelo MENOR custo?

A production database requires a sustained 16,000 IOPS and 500 MB/s throughput on a 500 GB volume. Which EBS volume type meets this requirement at the LOWEST cost?

A. io1
B. gp2
C. gp3
D. io2

---

40. Uma empresa determinou que sua carga de produção vai rodar na mesma família de instância EC2, no mesmo tamanho, na mesma região e no mesmo sistema operacional pelos próximos 3 anos, sem mudanças previstas. Qual opção de compra dá o MAIOR desconto sobre o preço sob demanda?

A company has determined that its production workload will run on the same EC2 instance family, size, Region, and operating system for the next 3 years with no anticipated changes. Which purchasing option provides the HIGHEST discount off On-Demand pricing?

A. Compute Savings Plans (prazo de 3 anos)
B. Instâncias reservadas padrão (prazo de 1 ano, sem pagamento adiantado)
C. Instâncias reservadas conversíveis (prazo de 3 anos, pagamento total adiantado)
D. Instâncias reservadas padrão (prazo de 3 anos, pagamento total adiantado)

---

41. Uma empresa compra instâncias reservadas (Reserved Instances) para uma carga de produção, mas prevê migrar nos próximos 18 meses para tipos de instância mais novos e econômicos, com possível mudança de família de instância e de sistema operacional. Qual tipo de instância reservada deve ser escolhido?

A company purchases Reserved Instances for a production workload but anticipates migrating to newer, more cost-efficient instance types within the next 18 months as they become available, potentially changing instance family and operating system. Which Reserved Instance type should be selected?

A. Instâncias reservadas conversíveis (Convertible Reserved Instances)
B. Instâncias reservadas padrão (Standard Reserved Instances)
C. Instâncias reservadas programadas (Scheduled Reserved Instances)
D. Instâncias reservadas zonais (Zonal Reserved Instances)

---

42. Um arquiteto de soluções quer reduzir os custos de armazenamento do EBS para uma carga de uso geral, garantindo uma base de 3.000 IOPS e 125 MiB/s de taxa de transferência, independentemente do tamanho do volume. Qual tipo de volume deve ser escolhido?

A solutions architect wants to reduce EBS storage costs for a general-purpose workload while still guaranteeing a baseline of 3,000 IOPS and 125 MiB/s throughput regardless of volume size. Which volume type should be selected?

A. gp3
B. gp2
C. io2 Block Express
D. st1

---

43. Uma empresa de mídia executa toda noite um trabalho em lote de transcodificação de vídeo que salva pontos de controle (checkpoints) do progresso e pode ser retomado se for interrompido. Minimizar o custo de computação é a principal prioridade. Qual opção de compra do EC2 é a MAIS econômica?

A media company runs a nightly video transcoding batch job that checkpoints progress and can resume if interrupted. Minimizing compute cost is the top priority for this workload. Which EC2 purchasing option is MOST cost-effective?

A. Hosts dedicados (Dedicated Hosts)
B. Instâncias reservadas (Reserved Instances)
C. Instâncias sob demanda (On-Demand)
D. Instâncias Spot

---

44. Uma empresa executa um banco de dados PostgreSQL de produção no Amazon RDS, em operação contínua, com uso previsível e estável no futuro próximo. Qual opção de compra MINIMIZA o custo desse banco de dados?

A company runs a production PostgreSQL database on Amazon RDS that operates continuously with predictable, steady-state usage for the foreseeable future. Which purchasing option MINIMIZES cost for this database?

A. Instâncias Spot para o RDS

B. Instâncias de banco de dados sob demanda (On-Demand)

C. RDS Serverless v2 provisionado com o máximo de ACUs

D. Instâncias reservadas do RDS (RDS Reserved Instances)

---

45. Uma empresa precisa reter registros de conformidade por 10 anos. Os registros são acessados cerca de uma vez por ano e, quando isso ocorre, os resultados precisam estar disponíveis em minutos, e não em horas. Qual classe de armazenamento do S3 tem o MENOR custo e ainda atende ao requisito de recuperação?

A company must retain compliance records for 10 years. The records are accessed roughly once per year, and when accessed, results must be available within minutes rather than hours. Which S3 storage class provides the LOWEST cost while meeting the retrieval requirement?

A. S3 Standard-IA

B. S3 Glacier Flexible Retrieval

C. S3 One Zone-IA

D. S3 Glacier Deep Archive

---

46. Uma empresa hospeda no Amazon S3 um conjunto de dados de pesquisa público, baixado com frequência por pesquisadores externos do mundo todo. A empresa quer que os usuários externos paguem a transferência de dados e os custos de requisição dos downloads, em vez do dono do bucket. Qual recurso do S3 deve ser ativado?

A company hosts a publicly available research dataset in Amazon S3 that is downloaded frequently by external researchers around the world. The company wants external users to pay for the download data transfer and request costs instead of the bucket owner. Which S3 feature should be enabled?

A. S3 Same-Region Replication

B. S3 Requester Pays

C. S3 Object Lock

D. S3 Transfer Acceleration

---

47. Uma empresa de mídia armazena milhões de objetos com padrões de acesso imprevisíveis e mutáveis: alguns objetos são acessados com frequência, outros ficam meses sem uso, e é impossível prever quais. Qual estratégia de armazenamento do S3 minimiza o custo com o MENOR esforço operacional?

A media company stores millions of objects with unpredictable, changing access patterns—some objects are accessed frequently, others go untouched for months, and it is impossible to predict which. Which S3 storage strategy minimizes cost with the LEAST operational overhead?

A. S3 Standard com uma regra de ciclo de vida que passe os objetos para o S3 Glacier Flexible Retrieval após 90 dias

B. S3 Intelligent-Tiering

C. S3 One Zone-IA para todos os objetos

D. S3 Standard com uma regra de ciclo de vida que passe os objetos para o S3 Standard-IA após 30 dias

---

48. Qual opção de pagamento de instâncias reservadas (Reserved Instances) oferece o MAIOR desconto em relação ao preço sob demanda para o mesmo prazo?

Which Reserved Instance payment option provides the LARGEST discount compared to On-Demand pricing for the same term length?

A. Sem pagamento adiantado (No Upfront)
B. Pagamento total adiantado (All Upfront)
C. Parcelas mensais sem compromisso
D. Pagamento parcial adiantado (Partial Upfront)

---

49. Qual modelo de preços do EC2 não exige pagamento adiantado nem compromisso de longo prazo e cobra por segundo nas instâncias Linux, o que o torna o mais indicado para cargas de curto prazo e imprevisíveis?

Which EC2 pricing model requires no upfront payment or long-term commitment and bills by the second for Linux instances, making it best suited for short-term, unpredictable workloads?

A. Instâncias sob demanda (On-Demand)
B. Instâncias Spot
C. Instâncias reservadas (Reserved Instances)
D. Savings Plans

---

50. Uma arquitetura replica dados toda noite de um bucket do S3 em us-east-1 para um bucket em eu-west-1, para recuperação de desastres, usando o S3 Cross-Region Replication. Qual custo o arquiteto de soluções deve considerar que NÃO se aplicaria com a Same-Region Replication?

An architecture replicates data nightly from an S3 bucket in us-east-1 to a bucket in eu-west-1 for disaster recovery using S3 Cross-Region Replication. Which cost should the solutions architect account for that would NOT apply with Same-Region Replication?

A. Cobranças de transferência de dados entre regiões
B. Cobranças de requisições PUT do S3
C. Cobranças de armazenamento do S3 no bucket de destino
D. Cobranças do S3 Replication Time Control

---

51. Um arquiteto de soluções quer uma solução de armazenamento do S3 que mova os objetos automaticamente entre camadas de acesso frequente e infrequente conforme o padrão de acesso muda, sem impacto no desempenho e sem regras de ciclo de vida manuais. Qual classe de armazenamento deve ser usada?

A solutions architect wants an S3 storage solution that automatically moves objects between frequent and infrequent access tiers based on changing access patterns, without performance impact or manual lifecycle rules. Which storage class should be used?

A. S3 One Zone-IA
B. S3 Standard-IA
C. S3 Glacier Instant Retrieval
D. S3 Intelligent-Tiering

---

52. Uma startup executa uma VPC de desenvolvimento de baixo tráfego, em que as instâncias de sub-redes privadas precisam de acesso de saída à internet, e quer minimizar o custo mensal. Qual opção é a forma MENOS cara de oferecer essa conectividade?

A startup runs a low-traffic development VPC that needs outbound internet access for private subnet instances and wants to minimize monthly cost. Which option is the LEAST expensive way to provide this connectivity?

A. Dois NAT Gateways para alta disponibilidade
B. AWS Direct Connect
C. Uma única instância NAT em um tipo de instância EC2 pequeno
D. Um NAT Gateway em cada zona de disponibilidade

Arquiteturas resilientes

53. Uma empresa de varejo quer criar uma arquitetura orientada a eventos em que atualizações de estoque de vários sistemas internos disparam ações independentes em diversos microsserviços downstream, com a capacidade de filtrar os eventos pelo conteúdo antes de rotear. Qual serviço da AWS é o MELHOR para o barramento de eventos?

A retail company wants to build an event-driven architecture where inventory updates from multiple internal systems trigger independent actions in several downstream microservices, with the ability to filter events by content before routing. Which AWS service is the BEST fit for the event bus?

A. Amazon SQS
B. Amazon EventBridge
C. AWS Step Functions
D. Amazon Kinesis Data Streams

---

54. Uma empresa de jogos executa em várias regiões da AWS uma aplicação multijogador baseada em TCP e sensível à latência, e precisa direcionar os jogadores ao endpoint mais saudável e de menor latência, oferecendo endereços IP anycast estáticos. Qual serviço o arquiteto de soluções deve usar?

A gaming company runs a latency-sensitive TCP-based multiplayer application across multiple AWS Regions and needs to route players to the healthiest, lowest-latency endpoint while providing static anycast IP addresses. Which service should the solutions architect use?

A. Roteamento baseado em latência do Amazon Route 53
B. AWS Global Accelerator
C. Balanceamento de carga entre zonas (cross-zone) do Elastic Load Balancing
D. Amazon CloudFront

---

55. Um banco de dados Amazon RDS for MySQL de produção está implantado em configuração Multi-AZ. O host subjacente na zona de disponibilidade primária sofre uma falha de hardware. O que acontece, do ponto de vista da aplicação, durante o failover automático?

A production Amazon RDS for MySQL database is deployed in a Multi-AZ configuration. The underlying host in the primary Availability Zone experiences a hardware failure. What occurs from the application's perspective during the automatic failover?

A. O endpoint (CNAME) da instância de banco de dados é atualizado para resolver para o standby, e a aplicação se reconecta sem mudar a string de conexão
B. O administrador do banco de dados precisa atualizar manualmente a string de conexão da aplicação para apontar para o standby
C. A réplica de leitura mais próxima na mesma região é promovida automaticamente a nova primária
D. As verificações de integridade do Amazon Route 53 detectam a falha e redirecionam o tráfego para o standby

---

56. Um arquiteto de soluções precisa projetar um banco de dados multirregional ativo-ativo para uma aplicação global que exige leituras e gravações de baixa latência em cada região, com resolução automática de conflitos. Qual solução atende a esse requisito?

A solutions architect must design a multi-region active-active database for a global application that requires low-latency reads and writes in each Region with automatic conflict resolution. Which solution meets this requirement?

A. Amazon ElastiCache for Redis com modo cluster ativado
B. Tabelas globais do Amazon DynamoDB
C. Implantação Multi-AZ do Amazon RDS
D. Réplicas de leitura do Amazon RDS em cada região

---

57. O aplicativo interno de relatórios de uma startup tolera até 24 horas de indisponibilidade e até 24 horas de perda de dados em caso de desastre regional. Minimizar o custo é a principal prioridade no desenho da recuperação de desastres. Qual estratégia é a MAIS adequada?

A startup's internal reporting application can tolerate up to 24 hours of downtime and up to 24 hours of data loss in the event of a regional disaster. Cost minimization is the top priority for the disaster recovery design. Which strategy is MOST appropriate?

A. Luz piloto (pilot light)
B. Multi-site ativo-ativo
C. Espera morna (warm standby)
D. Backup e restauração

---

58. A estratégia de recuperação de desastres de uma empresa mantém, o tempo todo, em uma região secundária, uma cópia reduzida, mas totalmente funcional, do ambiente de produção. Em uma interrupção regional, a empresa aumenta a escala do ambiente secundário para atender a todo o tráfego de produção. Qual é essa estratégia de recuperação de desastres?

A company's disaster recovery strategy runs a scaled-down but fully functional copy of its production environment in a secondary region at all times. During a regional outage, the company scales up the secondary environment to handle full production traffic. Which DR strategy is this?

A. Multi-site ativo-ativo
B. Espera morna (warm standby)
C. Luz piloto (pilot light)
D. Backup e restauração (backup and restore)

---

59. Um arquiteto de soluções projeta uma aplicação web de três camadas que deve continuar disponível se uma zona de disponibilidade inteira ficar indisponível. Qual escolha de arquitetura para a camada de banco de dados atende MELHOR a esse requisito?

A solutions architect is designing a three-tier web application that must remain available if an entire Availability Zone becomes unavailable. Which architecture choice for the database tier BEST meets this requirement?

A. Uma única instância do Amazon RDS com snapshots diários automáticos
B. Implantação Multi-AZ do Amazon RDS com um standby síncrono em uma segunda zona de disponibilidade
C. Amazon RDS com uma réplica de leitura na mesma zona de disponibilidade da primária
D. Implantação Single-AZ do Amazon RDS atrás de um Elastic Load Balancer

---

60. Um arquiteto de soluções projeta uma aplicação multirregional ativo-ativo com tabelas globais do Amazon DynamoDB. Dois usuários em regiões diferentes atualizam o mesmo item ao mesmo tempo, antes de a replicação terminar. Qual afirmação descreve corretamente como as tabelas globais do DynamoDB resolvem esse conflito?

A solutions architect is designing an active-active multi-region application using Amazon DynamoDB Global Tables. Two users in different regions update the same item simultaneously before replication completes. Which statement correctly describes how DynamoDB Global Tables resolves this conflict?

A. O DynamoDB aplica a regra 'a última gravação vence' (last-writer-wins), pelo horário de cada gravação, e propaga a mais recente para todas as tabelas réplica
B. O DynamoDB mescla os valores de atributos conflitantes em um único item com relógios vetoriais (vector clocks)
C. O DynamoDB rejeita as duas gravações e retorna uma ConditionalCheckFailedException aos dois clientes
D. O DynamoDB coloca as gravações conflitantes em fila e exige que a aplicação as resolva manualmente com uma função Lambda antes de a replicação continuar

---

61. Os requisitos de recuperação de desastres de uma empresa definem um RTO de 10 minutos e um RPO de 5 minutos para uma aplicação crítica de processamento de pedidos, com uma restrição de custo que descarta executar toda a capacidade de produção o tempo todo em uma segunda região. Qual estratégia de recuperação de desastres atende MELHOR a esses requisitos?

A company's disaster recovery requirements specify an RTO of 10 minutes and an RPO of 5 minutes for a critical order-processing application, with a cost constraint that rules out running full production capacity continuously in a second region. Which DR strategy BEST satisfies these requirements?

A. Luz piloto, mantendo ativa só a replicação do banco central e montando a capacidade de computação do zero durante um desastre

B. Espera morna, executando na segunda região uma cópia reduzida, mas totalmente funcional, da carga, que pode ser escalada rapidamente

C. Backup e restauração, copiando snapshots para uma segunda região a cada 6 horas com o AWS Backup

D. Multi-site ativo-ativo, executando toda a capacidade de produção nas duas regiões ao mesmo tempo, o tempo todo

---

62. Uma empresa de jogos precisa de um banco de dados NoSQL que replique os dados automaticamente entre várias regiões da AWS com gravações multiativas, para que jogadores de qualquer região tenham leituras e gravações de baixa latência, com consistência eventual entre regiões. Qual solução atende MELHOR a esse requisito?

A gaming company needs a NoSQL database that automatically replicates data across multiple AWS Regions with multi-active writes, so players in any Region experience low-latency reads and writes with eventual consistency across Regions. Which solution BEST meets this requirement?

A. Amazon DynamoDB com um índice secundário global (Global Secondary Index)

B. Amazon ElastiCache for Redis com modo cluster ativado

C. Tabelas globais do Amazon DynamoDB (global tables)

D. Amazon RDS Multi-AZ com réplicas de leitura entre regiões

---

63. Um arquiteto de soluções projeta uma camada de cache que deve fazer failover automático para um nó réplica em segundos, se o nó primário ficar indisponível, sem exigir nenhuma intervenção no nível da aplicação. Qual configuração do ElastiCache atende a esse requisito?

A solutions architect is designing a caching layer that must automatically fail over to a replica node within seconds if the primary node becomes unavailable, without requiring any application-level intervention. Which ElastiCache configuration meets this requirement?

A. Amazon ElastiCache for Redis com modo cluster desativado e sem nós réplica

B. Amazon ElastiCache for Memcached com Auto Discovery ativado em vários nós

C. Amazon ElastiCache for Redis com Multi-AZ ativado e pelo menos uma réplica de leitura

D. Amazon ElastiCache for Memcached implantado em várias zonas de disponibilidade, com um único nó por zona

---

64. Uma empresa de serviços financeiros exige uma solução de recuperação de desastres entre regiões para seu banco de dados Amazon Aurora MySQL, com RPO abaixo de 1 segundo e RTO abaixo de 1 minuto em uma interrupção regional. Qual solução atende MELHOR a esses requisitos?

A financial services firm requires a cross-region disaster recovery solution for its Amazon Aurora MySQL database with an RPO under 1 second and an RTO under 1 minute during a regional outage. Which solution BEST meets these requirements?

A. Backups automáticos do Aurora replicados para uma região secundária com o AWS Backup

B. AWS Database Migration Service com replicação contínua para uma região secundária

C. Implantação Multi-AZ do Amazon RDS com uma réplica de leitura entre regiões

D. Amazon Aurora Global Database com uma região secundária

---

65. Um arquiteto de soluções explica a infraestrutura global da AWS a um novo membro da equipe. Qual afirmação descreve MELHOR uma zona de disponibilidade (AZ)?

A solutions architect is explaining AWS global infrastructure to a new team member. Which statement BEST describes an Availability Zone (AZ)?

A. Um agrupamento lógico de buckets do Amazon S3 replicados entre países

B. Um único rack de servidor físico dedicado a uma conta de cliente

C. Um ou mais data centers distintos, com energia, rede e conectividade redundantes, dentro de uma região da AWS

D. Uma coleção geograficamente isolada de regiões da AWS, ligadas por links de baixa latência

---

66. Uma empresa executa uma aplicação de gerenciamento de conteúdo em instâncias EC2 que precisam compartilhar um sistema de arquivos comum, com os mesmos arquivos acessíveis e graváveis, ao mesmo tempo, por instâncias de várias zonas de disponibilidade. Qual solução de armazenamento atende MELHOR a esse requisito?

A company runs a content management application on EC2 instances that must share a common file system, with the same files accessible and writable from instances in multiple Availability Zones simultaneously. Which storage solution BEST meets this requirement?

A. Volumes Amazon Instance Store (armazenamento da instância), replicados por um script personalizado

B. Volume Amazon EBS anexado a várias instâncias com Multi-Attach em uma única zona de disponibilidade

C. Amazon EFS com destinos de montagem em cada zona de disponibilidade

D. Bucket do Amazon S3 montado com um driver FUSE personalizado

---

67. Uma aplicação com tabela global do DynamoDB multirregional permite gravações no mesmo item em us-east-1 e eu-west-1 quase ao mesmo tempo. Com qual comportamento de resolução de conflitos o arquiteto deve planejar o desenho?

A multi-Region DynamoDB Global Table application allows writes to the same item in both us-east-1 and eu-west-1 nearly simultaneously. What conflict resolution behavior should the architect design around?

A. O DynamoDB mescla as duas gravações no item com um relógio vetorial (vector clock) e retorna o resultado mesclado

B. O DynamoDB bloqueia as gravações na tabela réplica até que um administrador resolva o conflito

C. O DynamoDB rejeita a segunda gravação e retorna uma ConditionalCheckFailedException ao cliente

D. O DynamoDB aplica a regra 'a última gravação vence' (last-writer-wins) com base em horários internos, e a gravação mais recente entre as regiões é mantida

---

68. Uma empresa precisa de alta disponibilidade com failover em menos de um minuto E da capacidade de transferir consultas de relatórios com muita leitura para um standby legível, sem afetar a primária. Qual implantação do RDS atende MELHOR aos dois requisitos?

A company needs both high availability with sub-minute failover AND the ability to offload read-heavy reporting queries to a readable standby without impacting the primary. Which RDS deployment BEST satisfies both requirements?

A. Um cluster de banco de dados Multi-AZ do RDS com duas instâncias standby legíveis

B. Uma única instância do RDS com backups automáticos e cópia de snapshot Multi-AZ

C. Uma única instância do RDS com duas réplicas de leitura entre regiões

D. Uma implantação Multi-AZ clássica do RDS com um standby que não é legível

---

69. Um arquiteto de soluções implantou um banco de dados Amazon RDS MySQL com Multi-AZ ativado. A instância primária do banco fica inacessível por uma falha de hardware subjacente. O que acontece com a conectividade de banco de dados da aplicação?

A solutions architect deployed an Amazon RDS MySQL database with Multi-AZ enabled. The primary database instance becomes unreachable due to an underlying hardware failure. What happens to the application's database connectivity?

A. O RDS faz o failover automático para a instância standby em outra AZ, e o endpoint do banco de dados permanece o mesmo

B. O RDS faz o failover automático para uma réplica de leitura, e a aplicação precisa atualizar a string de conexão

C. O RDS cria uma nova instância primária na mesma AZ, causando uma breve interrupção até o DNS se propagar

D. A aplicação precisa promover manualmente a instância standby pela AWS CLI

Resposta correta

1. D O Elastic Fabric Adapter é uma interface de rede construída sobre o ENA que adiciona uma interface de hardware com bypass do sistema operacional. Aplicações que usam bibliotecas MPI ou NCCL se comunicam com latência menor e mais consistente que a pilha TCP/IP do kernel, o que é ideal para clusters de HPC fortemente acoplados. O ENA padrão oferece alta largura de banda, mas o tráfego ainda passa pelo kernel. Uma segunda ENI só cria outro caminho de rede. O Global Accelerator otimiza o tráfego de clientes externos, não a comunicação entre nós do cluster.

2. B O DAX é um cache em memória totalmente gerenciado e compatível com o DynamoDB, que exige apenas pequenas mudanças no código (trocar o cliente) e entrega respostas em microssegundos para cargas com muita leitura ou picos. O ElastiCache for Redis é um cache de uso geral, mas obriga a aplicação a gerenciar a lógica de cache e a invalidação, uma complexidade que o DAX evita. Aumentar as RCUs melhora a capacidade, mas não reduz a latência por requisição a microssegundos. As Global Tables tratam de replicação multirregional, não de latência de leitura.

3. C O Lambda cobra só pelo tempo real de execução, escala sozinho para picos imprevisíveis e não exige gerenciar servidores, o que o torna ideal para trabalhos curtos (dentro do limite de 15 minutos) e irregulares. As instâncias reservadas cobram a capacidade contínua mesmo ociosa. Um Auto Scaling com mínimo de uma instância gera custo mesmo sem uso e exige gerenciar patches e escala. O Lightsail com instância fixa não escala sozinho e cobra de forma contínua, o que não combina com cargas em picos.

4. A Só o io2 Block Express oferece até 256.000 IOPS e 4.000 MB/s por volume, com latência abaixo de um milissegundo. O gp3 chega a 80.000 IOPS e 2.000 MiB/s, o que não basta. Os limites do io2 antigo, sem Block Express, eram 64.000 IOPS e 1.000 MiB/s; os volumes io2 atuais usam Block Express. O st1 é um HDD otimizado para taxa de transferência em cargas sequenciais grandes, como processamento de logs, e o striping não muda sua latência maior nem o torna competitivo em IOPS com os volumes SSD.

5. B O S3 Transfer Acceleration encaminha os uploads pelo ponto de presença (edge location) mais próximo do CloudFront e pela rede de backbone otimizada da AWS até o bucket, melhorando bastante a taxa de transferência para quem envia de longe. Uma distribuição do CloudFront também pode acelerar uploads para uma origem, mas o Transfer Acceleration foi feito para uploads distribuídos direto ao S3. O upload multipart melhora a confiabilidade e o paralelismo de um cliente, mas não o caminho de rede entre continentes. A replicação só copia os dados depois.

6. A No Aurora MySQL, as réplicas compartilham o mesmo volume de armazenamento do cluster da instância primária, então o atraso de replicação costuma ser de dezenas de milissegundos, e o Aurora oferece até 15 réplicas por cluster. O RDS for MySQL com réplicas de leitura também aceita até 15, mas usa replicação assíncrona por binlog, sem armazenamento compartilhado. A instância standby do Multi-AZ no RDS for MySQL não é legível e serve só para failover. O DAX é um cache do DynamoDB e não se aplica a uma carga relacional MySQL.

7. C O io2 Block Express entrega até 256.000 IOPS e latência abaixo de um milissegundo, com durabilidade de 99,999%, e foi feito para bancos de dados intensivos em E/S e sensíveis à latência. O SSD de uso geral (gp3) chega a 80.000 IOPS provisionados, o que não basta. O st1 e o sc1 são volumes HDD otimizados para taxa de transferência em cargas sequenciais grandes (big data, processamento de logs), não para IOPS aleatório alto, e têm limites de IOPS muito abaixo do que um banco transacional precisa.

8. D O Amazon CloudFront é uma rede de distribuição de conteúdo (CDN) que guarda o conteúdo em cache em pontos de presença distribuídos pelo mundo e atende às requisições a partir do ponto mais próximo, o que reduz a latência dos usuários. O ElastiCache guarda em memória dados de aplicação e de banco para a computação de back-end, não entrega conteúdo aos usuários finais. O Direct Connect oferece um link privado dedicado até a AWS, sem cache nem distribuição de conteúdo. O Route 53 é um DNS que pode rotear tráfego, mas não guarda conteúdo em cache.

9. D O Origin Shield adiciona uma camada extra de cache entre os caches regionais do CloudFront e a origem, consolidando as requisições de vários pontos de presença em um único cache antes de chegarem à origem. Isso reduz bastante a carga na origem e melhora a taxa de acerto do cache para tráfego global. A criptografia em nível de campo protege dados sensíveis e não afeta o cache. As URLs assinadas controlam o acesso. Os gatilhos do Lambda@Edge permitem alterar requisições antes da origem, mas não reduzem as buscas independentes de cada ponto.

10. C O Origin Shield adiciona uma camada de cache centralizada entre os pontos de presença e a origem e consolida as requisições de vários pontos em uma só ida à origem em um cache miss, o que reduz a carga de forma direta. Aumentar a capacidade da origem trata o sintoma, não a causa, e adiciona custo contínuo. Aumentar o TTL foi excluído de forma explícita, por ser uma mudança de estratégia, e ainda arrisca servir conteúdo desatualizado. O Lambda@Edge executa lógica personalizada nos pontos de presença, mas não consolida as buscas na origem.

11. C O Amazon S3 oferece pelo menos 3.500 requisições PUT/COPY/POST/DELETE e 5.500 GET/HEAD por segundo por prefixo particionado; distribuir os objetos em vários prefixos de chave aumenta o throughput de requisições, pois permite acesso paralelo entre os prefixos. Essas taxas são bases suportadas, não limites máximos fixos, e o S3 escala aos poucos conforme a taxa aumenta. O Transfer Acceleration acelera transferências a longa distância, não o processamento por prefixo. O Standard-IA muda custo e recuperação, e o Versioning não afeta a taxa de requisições.

12. B Os volumes io2 (e io1) aceitam o Multi-Attach, que permite anexar o mesmo volume a até 16 instâncias baseadas em Nitro em uma única zona de disponibilidade, para acesso simultâneo em nível de bloco, com sistemas de arquivos que reconhecem clusters e baixa latência. O EFS dá acesso compartilhado em nível de arquivo, não armazenamento em blocos. O S3 com Transfer Acceleration acelera uploads de objetos a longa distância. O gp3 não aceita Multi-Attach e não atende várias instâncias ao mesmo tempo.

13. A Os grupos de posicionamento em cluster agrupam as instâncias bem próximas em uma única zona de disponibilidade, com rede de baixa latência e alta taxa de transferência, ideal para HPC e cargas MPI fortemente acopladas. Os grupos distribuídos (spread) espalham as instâncias por hardware distinto para reduzir falhas correlacionadas, não para otimizar a latência entre elas. Os grupos por partição isolam conjuntos de instâncias para limitar o impacto de falhas em sistemas como Hadoop e Cassandra. O posicionamento padrão não garante latência nem proximidade.

14. C O Amazon ElastiCache é um armazenamento em memória totalmente gerenciado (Redis ou Memcached), feito para guardar em cache dados de aplicação e resultados de consultas de banco, reduzindo a latência de leitura de milissegundos para microssegundos. O DAX só serve para o DynamoDB, não para bancos relacionais como o RDS. O CloudFront guarda conteúdo em cache nos pontos de presença para web e API, não resultados de consultas. O Storage Gateway liga o armazenamento local à AWS e não faz cache de leituras de banco.

15. C O Memcached é multithread e escala por vários núcleos em um único nó, o que o torna adequado para cache simples e de alta vazão de dados de sessão, sem necessidade de persistência, replicação ou estruturas de dados complexas. O Redis tem uma thread por shard e oferece durabilidade e tipos de dados avançados, melhor para casos com persistência ou pub/sub, não para vazão bruta em vários núcleos. O DAX é uma camada de cache exclusiva do DynamoDB. O RDS Proxy agrupa conexões de banco e não é um cache em memória.

16. A O Memcached tem arquitetura multithread, que escala de forma nativa por todos os núcleos de CPU de um nó e maximiza a vazão por nó em um cache simples de chave e valor, sem persistência. O Redis executa comandos em uma única thread por shard; o modo cluster ativado escala na horizontal ao dividir os dados em shards entre vários nós. O ElastiCache for Redis pode usar threads extras para E/S aprimorada, mas isso não torna multithread a execução de comandos. Multi-AZ e failover adicionam replicação desnecessária e não paralelizam os comandos.

17. A O CloudFront com o bucket do S3 como origem guarda o conteúdo em cache nos pontos de presença, então os usuários da Ásia o recebem de um ponto próximo, e não de us-east-1, com configuração simples e gerenciada. O Transfer Acceleration acelera transferências a longa distância, mas não guarda objetos em cache perto dos usuários. A replicação entre regiões traz muita complexidade operacional e ainda exige roteamento. Não há instância EC2 neste cenário estático para redimensionar.

18. C O limite de permissões (permissions boundary) é uma política gerenciada que define o máximo de permissões que uma entidade do IAM pode ter: as permissões efetivas são a interseção entre as políticas baseadas em identidade e o limite. Mesmo que o desenvolvedor anexe uma política permissiva demais, as ações fora do limite são negadas. As SCPs valem no nível da conta ou da OU e são geridas por administradores do Organizations, não por função na hora da criação. As políticas de grupo não limitam as anexadas direto à função, e as baseadas em recurso controlam o acesso por recurso.

19. C As funções do IAM (IAM roles) anexadas por perfil de instância (instance profile) dão credenciais temporárias, com rotação automática, entregues pelo serviço de metadados da instância, sem guardar credenciais nela. Isso segue o privilégio mínimo e reduz a exposição se a instância for comprometida. Guardar chaves em variáveis de ambiente ou no código cria segredos de longo prazo que podem vazar, e as credenciais raiz nunca devem ser usadas por aplicações. A AWS recomenda funções, e não credenciais estáticas, para EC2, Lambda ou tarefas do ECS.

20. C O AWS Shield Advanced é um nível pago que acrescenta acesso 24 horas por dia à equipe de resposta a DDoS da AWS, detecção e mitigação avançadas de ataques e créditos de proteção de custos pelas cobranças de escala de um evento DDoS. O Shield Standard é gratuito e automático, mas só dá proteção básica nas camadas de rede e transporte, sem a DRT nem proteção de custos. As regras baseadas em taxa do WAF limitam inundações de requisições na camada 7, sem a DRT nem créditos. O GuardDuty detecta ameaças e não mitiga DDoS.

21. D Ativar a criptografia do EBS por padrão no nível da conta e da região criptografa automaticamente com uma chave do KMS todos os volumes novos e os snapshots derivados deles, sem ação por volume. A criptografia manual com ferramentas de terceiros aumenta o esforço operacional e o risco de esquecer volumes. Os snapshots do EBS não ficam em um bucket do S3 acessível ao cliente, então a criptografia padrão do S3 não os afeta. Uma política de negação sem ativar o recurso só bloquearia a criação de volumes, sem criptografar nada.

22. D O SSE-KMS se integra ao AWS CloudTrail e registra cada chamada de API do KMS, como Decrypt e GenerateDataKey, com o principal que a fez, gerando uma trilha de auditoria detalhada por objeto. O SSE-S3 usa chaves gerenciadas pela AWS, sem visibilidade no CloudTrail sobre o uso de cada chave. A criptografia no cliente com chave local tira da AWS a capacidade de auditar o uso da chave. No SSE-C o cliente fornece a chave em cada requisição, e isso não gera os mesmos registros do CloudTrail baseados no KMS.

23. D Os endpoints de gateway do S3 só são alcançáveis por recursos dentro da VPC, por entradas na tabela de rotas, e não podem ser acessados de redes locais por Direct Connect ou VPN. Um endpoint de interface (AWS PrivateLink) cria ENIs com IPs privados na VPC, alcançáveis pelo Direct Connect, o que permite acesso privado ao S3 a partir do ambiente local, sem exposição à internet. O Transfer Acceleration otimiza a velocidade pela internet pública, o oposto do requisito. Adicionar um internet gateway anula o objetivo de evitar o trânsito pela internet pública.

24. B O NAT gateway reescreve o IP de origem para o seu próprio Elastic IP público, que fica fora do CIDR permitido: o endpoint do S3 voltado à internet enxerga o IP público, e não um endereço de 10.20.0.0/16. Rotear por um endpoint de VPC de gateway, com condições aws:sourceVpce ou aws:SourceVpc, manteria o escopo pretendido. O aws:SourceIp é avaliado normalmente no tráfego roteado pela internet, então a ideia de que ele não funciona para tráfego de VPC é falsa. O CORS trata de requisições entre origens em navegadores, e o aws:SourceIp não se limita a IPv6.

25. D O AWS Shield é um serviço gerenciado de proteção contra DDoS; o Standard é ativado automaticamente, sem custo, para todos os clientes, e o Advanced acrescenta detecção avançada e acesso 24 horas à equipe de resposta a DDoS para ataques nas camadas 3/4 e 7. O AWS WAF filtra e bloqueia requisições HTTP/HTTPS maliciosas (injeção de SQL, XSS), mas sozinho não é um serviço específico de mitigação de DDoS. O Firewall Manager gerencia de forma central essas proteções entre contas, sem ser o mecanismo. O GuardDuty detecta ameaças analisando logs e não mitiga.

26. C O SSE-KMS com o CloudTrail registra as chamadas de API do KMS, como GenerateDataKey e Decrypt, e identifica quem chamou e quando. Ele pode usar uma chave gerenciada pela AWS ou pelo cliente; as S3 Bucket Keys reduzem as chamadas ao KMS, então a auditoria por objeto exige deixá-las desativadas. O SSE-S3 não mostra o uso de cada chave. A criptografia no cliente com chave embutida não tem auditoria central, e o SSE-C não registra o uso pelo KMS.

27. C O AWS KMS foi feito para criar, gerenciar e controlar chaves criptográficas (CMKs), com rotação de chaves e políticas de chave detalhadas, usadas na criptografia SSE-KMS de objetos do S3. O AWS Secrets Manager guarda e rotaciona segredos de aplicação, como credenciais de banco, não chaves de criptografia. O ACM emite e gerencia certificados SSL/TLS para proteger o tráfego de rede, não objetos. O Parameter Store guarda valores de configuração e segredos como parâmetros de texto, sem gerenciar chaves criptográficas usadas para criptografar dados.

28. D Conceder s3:GetObject e s3:PutObject restritos a arn:aws:s3:::company-bucket/dev-uploads/* dá só as ações necessárias e limita o ARN do recurso ao prefixo exato, o que atende ao privilégio mínimo. A AmazonS3FullAccess dá acesso irrestrito a todos os buckets e ações da conta, muito além do necessário. O curinga s3:* concede permissões desnecessárias, como DeleteObject; ações de bucket, como DeleteBucket e PutBucketPolicy, não se aplicam a esse ARN de objeto. Resource "*" dá acesso no IAM a todos os buckets e objetos da conta, mesmo com uma bucket policy.

29. B A lógica de avaliação de políticas do IAM segue uma ordem rígida: uma negação explícita em qualquer política aplicável, anexada ao usuário, a um grupo ou a uma função, sempre prevalece sobre qualquer permissão, não importa de onde ela venha. Não existe a ideia de políticas de usuário valerem mais que as de grupo, e o IAM não avalia políticas pela data de anexação. A origem da negação (grupo ou usuário) não muda o resultado: a negação explícita é decisiva nos dois casos.

30. A O KMS é único entre os serviços da AWS porque sempre exige uma instrução de política de chave, baseada em recurso, como âncora de confiança. No acesso entre contas, a política de chave da CMK na conta proprietária precisa autorizar de forma explícita a conta ou o principal externo, além da política do IAM dele; sem isso, a permissão do IAM sozinha não autoriza o uso da chave. Um Resource curinga no IAM é questão de boas práticas, não a causa da negação. As concessões são outro mecanismo, não um requisito. As bucket policies do S3 não regem ações do KMS.

31. D A criptografia de envelope usa o KMS para gerar uma chave de dados única por objeto: a chave de dados em texto simples criptografa o objeto localmente, e depois a própria chave de dados é criptografada pela chave mestra do cliente (CMK) do KMS e guardada junto com o texto cifrado. Isso evita enviar grandes volumes de dados ao KMS, cujas operações têm limite de tamanho, e centraliza o controle da CMK. Criptografar o objeto inteiro direto não é possível por esse limite. A CMK não guarda o objeto, e a chave de dados vem da API GenerateDataKey do KMS.

32. C O AWS Secrets Manager oferece modelos prontos de rotação com Lambda para RDS, Redshift e DocumentDB e permite a rotação automática agendada, como a cada 30 dias. O Parameter Store guarda valores SecureString, mas não tem fluxo nativo de rotação automática de credenciais de banco sem automação personalizada. A rotação automática do KMS troca o material da chave de criptografia, uma vez por ano, e não tem relação com senhas de banco. A autenticação do IAM troca senhas estáticas por tokens de curta duração, um mecanismo diferente.

33. B Os VPC Flow Logs capturam metadados do tráfego IP de e para as interfaces de rede de uma VPC, incluindo IP de origem e destino, porta, protocolo e se o tráfego foi ACCEPT ou REJECT segundo as regras dos security groups e das NACLs. O CloudTrail registra chamadas de API, não o fluxo de pacotes, e não mostraria IPs de origem chegando a uma ENI. O AWS Config acompanha mudanças de configuração, não tráfego ao vivo. O Inspector avalia vulnerabilidades e exposição de cargas, não registra tráfego.

34. A O AWS Network Firewall aceita regras com estado baseadas em domínio (FQDN), que filtram o tráfego HTTP/HTTPS de saída pelo nome do host, e não pelo IP, o que é essencial quando os IPs de destino mudam com frequência, como atrás de uma CDN ou de um balanceador. Os security groups e as NACLs só filtram por IP/CIDR e porta e não conhecem nomes de domínio, exigiriam atualização manual constante e não são confiáveis em escala. A política de um endpoint de gateway controla o acesso ao S3 ou ao DynamoDB, não o tráfego para domínios de um parceiro na internet.

35. B A criptografia de armazenamento do RDS não pode ser ligada em uma instância existente: é uma propriedade imutável definida só na criação. O caminho suportado é fazer um snapshot do banco não criptografado, copiá-lo informando uma chave KMS (o que gera uma cópia criptografada) e restaurar uma nova instância a partir do snapshot criptografado, depois fazer a troca. Modificar ou reiniciar a instância ativa não oferece essa opção. Uma primária não criptografada não gera réplica criptografada, pois a réplica herda o estado de criptografia da origem.

36. B As instâncias Spot usam capacidade ociosa do EC2 e podem dar descontos de até 90% sobre o preço sob demanda, o que as torna ideais para cargas flexíveis e tolerantes a falhas, como processamento em lote, pois a AWS pode retomar a capacidade com aviso de interrupção de dois minutos. As instâncias reservadas padrão exigem compromisso de 1 ou 3 anos, cobrado independentemente da tolerância a interrupção. As instâncias sob demanda têm o maior custo por hora, sem desconto. Os hosts dedicados são cobrados por servidor físico, para conformidade e licenciamento.

37. A As instâncias reservadas padrão com prazo de 3 anos dão o maior desconto, de até cerca de 72% sobre o preço sob demanda, para cargas previsíveis e de estado estável, pois o cliente se compromete com uma configuração fixa pelo maior prazo. O preço sob demanda não tem desconto e serve a cargas imprevisíveis. As instâncias Spot são mais baratas, mas podem ser interrompidas e não servem para um banco sempre ligado. As conversíveis de 1 ano permitem trocar a família de instância, mas rendem desconto menor que o das padrão de 3 anos.

38. A O CloudFront com Origin Access Control guarda o conteúdo em cache nos pontos de presença, então as requisições repetidas não voltam ao S3. A transferência do S3 para o CloudFront é gratuita, e o preço de saída do CloudFront costuma ser menor que o da saída direta do S3, o que reduz custo e latência. O Transfer Acceleration cobra uma taxa extra em vez de reduzir a saída. O One Zone-IA reduz o custo de armazenamento, não o de transferência. Replicar para todas as regiões multiplica custos.

39. C Os volumes gp3 têm uma base de 3.000 IOPS e 125 MB/s incluída no preço base, com desempenho provisionado independente do tamanho do volume. Os limites atuais do gp3 chegam a 80.000 IOPS e 2.000 MiB/s, conforme o volume e a instância. Um gp3 de 500 GB sustenta os 16.000 IOPS e 500 MB/s exigidos por um custo menor que o do io1 ou do io2. O io1 e o io2 cobram um adicional por IOPS provisionado; o io2 ainda oferece mais durabilidade. No gp2, o IOPS cresce com o tamanho (3 IOPS por GB) e não sustenta esse requisito em 500 GB sem superdimensionar muito.

40. D As instâncias reservadas padrão com prazo de 3 anos e pagamento total adiantado oferecem o maior desconto entre as opções listadas, de até cerca de 72% sobre o preço sob demanda. Como família, região e sistema operacional ficam fixos pelo prazo todo, não há motivo para aceitar o desconto menor das conversíveis por uma flexibilidade que não será usada. Os Compute Savings Plans dão descontos próximos, mas em geral um pouco menores. A reservada de 1 ano sem pagamento adiantado rende bem menos.

41. A As instâncias reservadas conversíveis podem ser trocadas durante o prazo por outra família, tamanho, sistema operacional ou locação, desde que a troca tenha valor igual ou maior, o que serve a quem prevê migrar. As padrão não podem mudar de família e só admitem mudanças limitadas, como a AZ, o que prende a empresa a um tipo que ela pretende abandonar. 'Zonais' não é uma opção de compra à parte: as RIs apenas têm escopo regional ou de zona de disponibilidade. As programadas, uma oferta descontinuada, serviam a capacidade recorrente em janelas de tempo.

42. A Os volumes SSD de uso geral gp3 oferecem uma base de 3.000 IOPS e 125 MiB/s independente do tamanho do volume, por um preço por GB menor que o do gp2, e deixam provisionar IOPS ou taxa de transferência extras em separado, sem superdimensionar o volume. No gp2, o desempenho base cresce com o tamanho do volume, o que muitas vezes obriga a superdimensionar a capacidade para ter IOPS suficiente, e aumenta o custo. O io2 Block Express serve a cargas críticas de IOPS alto, por um preço maior. O st1 é um HDD para cargas sequenciais grandes, não de uso geral.

43. D As instâncias Spot dão descontos de até 90% sobre o preço sob demanda e são ideais para cargas em lote tolerantes a falhas e a interrupções, como transcodificações com checkpoint que podem ser retomadas. As instâncias reservadas exigem compromisso de 1 ou 3 anos, o que combina mal com uma carga que roda pouco tempo por noite. As sob demanda têm o maior custo por hora, sem desconto. Os hosts dedicados são precificados para conformidade e licenciamento, não para economia, e são a opção mais cara aqui.

44. D As instâncias reservadas do RDS dão descontos de até 69% sobre o preço sob demanda em troca de compromisso de 1 ou 3 anos, o que combina bem com o uso previsível e estável de um banco de dados. O preço sob demanda não dá desconto para uso contínuo. O Amazon RDS não tem modelo de compra Spot: essa opção é exclusiva do EC2 e não existe para o RDS gerenciado. Manter o Aurora Serverless v2 fixo na capacidade máxima elimina o benefício de custo do escalonamento automático e costuma custar mais que uma reservada bem dimensionada.

45. B O S3 Glacier Flexible Retrieval oferece recuperação acelerada (expedited) em 1 a 5 minutos e tem preço bem menor que o Standard-IA para dados de arquivo raramente acessados, o que atende ao requisito de 'uma vez por ano, em minutos' pelo menor custo. O Deep Archive é mais barato por GB, mas sua recuperação padrão leva cerca de 12 horas, e não atende ao requisito de minutos. O Standard-IA e o One Zone-IA foram feitos para acesso mensal, não anual, e custam mais por GB armazenado que as camadas Glacier nesse padrão de acesso.

46. B O S3 Requester Pays transfere os custos de transferência de dados e de requisições do dono do bucket para quem baixa os objetos, e foi feito para cenários em que terceiros acessam conjuntos de dados compartilhados ou públicos. O Object Lock impõe retenção do tipo grava uma vez, lê várias (WORM) para conformidade e não transfere custos. O Transfer Acceleration acelera transferências a distância, mas o dono do bucket continua pagando, com taxa extra. A Same-Region Replication duplica dados e não muda quem paga os downloads.

47. B O S3 Intelligent-Tiering monitora o acesso por objeto e o move entre as camadas frequente, infrequente e de arquivo, sem taxas de recuperação e com pouco esforço operacional, o que é ideal para acesso imprevisível. As regras de ciclo de vida para Standard-IA ou Glacier exigem acertar quando o objeto será acessado, e geram taxas de recuperação e cobrança de duração mínima. O One Zone-IA abre mão da resiliência entre AZs. A pequena taxa de monitoramento pode ser superada pela economia.

48. B As instâncias reservadas com pagamento total adiantado exigem o custo inteiro no início, e em troca a AWS dá o maior desconto sobre o preço sob demanda para aquele prazo, pois recebe tudo de imediato. O pagamento parcial adiantado exige um valor inicial menor e cobra o restante por hora, com desconto um pouco menor. A opção sem pagamento adiantado não exige nada no início e é cobrada por hora durante o prazo, dando o menor desconto das três. 'Parcelas mensais sem compromisso' não é uma opção real de pagamento de RI e descreve a cobrança sob demanda.

49. A As instâncias sob demanda permitem pagar pela capacidade de computação por segundo no Linux, ou por hora, sem pagamento adiantado nem contrato de longo prazo, o que serve a cargas com picos, imprevisíveis ou curtas, como testes de desenvolvimento. As instâncias reservadas e os Savings Plans exigem compromisso de 1 ou 3 anos em troca de desconto, o que não serve a necessidades de curto prazo e imprevisíveis. As instâncias Spot também têm pouco compromisso, mas podem ser interrompidas com aviso de dois minutos, risco que a sob demanda não tem.

50. A O Cross-Region Replication copia objetos de um bucket em uma região para um bucket em outra e gera a cobrança padrão de transferência de dados entre regiões, por GB, de cada objeto replicado, uma cobrança que não existe na Same-Region Replication, pois o tráfego nunca sai da região. As cobranças de requisição PUT e de armazenamento no destino valem para os dois tipos, pois ambos gravam e guardam as réplicas. O Replication Time Control é um complemento opcional disponível nos dois, e não distingue um do outro.

51. D O S3 Intelligent-Tiering monitora automaticamente os padrões de acesso e move os objetos entre suas camadas de acesso instantâneo, sem impacto no desempenho nem taxas de recuperação, o que é ideal quando o padrão de acesso é desconhecido ou muda. Suas camadas opcionais Archive Access e Deep Archive Access exigem restauração antes do acesso. O S3 Standard-IA exige saber de antemão que os dados são pouco acessados e cobra taxa de recuperação. O One Zone-IA usa uma só AZ, e o Glacier Instant Retrieval é uma camada fixa; nenhum move objetos sozinho.

52. C Uma instância NAT pequena só gera o custo normal da instância EC2 mais a transferência de dados, o que costuma sair mais barato, em ambientes de desenvolvimento de baixo tráfego e não críticos, que a cobrança por hora do NAT Gateway somada à taxa por GB processado. Os NAT Gateways, ainda mais um por AZ, são gerenciados e altamente disponíveis, mas custam mais e fazem sentido na produção. O Direct Connect liga à infraestrutura local, não dá saída à internet e é bem mais caro.

53. B O Amazon EventBridge é um barramento de eventos serverless, feito para rotear eventos de várias origens para vários destinos com regras de filtragem por conteúdo, o que o torna ideal para fan-out e arquiteturas de microsserviços orientadas a eventos. O Amazon SQS é uma fila ponto a ponto, sem filtragem nativa por conteúdo para vários destinos. O AWS Step Functions orquestra fluxos de trabalho, não roteia eventos independentes. O Kinesis Data Streams serve a análise de streaming de alto volume, não ao roteamento de eventos por regras.

54. B O AWS Global Accelerator usa a rede global da AWS e IPs anycast estáticos para rotear tráfego TCP/UDP ao melhor endpoint saudável entre regiões, por latência e integridade, o que serve a cargas sensíveis à latência que não são HTTP, como jogos. O CloudFront é otimizado para cache HTTP/HTTPS, não para roteamento TCP. O roteamento por latência do Route 53 atua no DNS e reage mais devagar à integridade do endpoint. O balanceamento entre zonas distribui tráfego dentro de um balanceador, não entre regiões.

55. A O failover Multi-AZ do RDS muda o registro DNS por trás do endpoint fixo da instância para apontar para o standby, que passa a ser a nova primária em outra AZ; a aplicação só se reconecta quando a entrada DNS se propaga, sem mudar código nem configuração. As verificações de integridade do Route 53 não fazem parte do mecanismo interno de failover do RDS. Não se edita a string de conexão à mão. As réplicas de leitura são cópias assíncronas separadas e não são promovidas automaticamente no failover Multi-AZ; só o standby síncrono designado é promovido.

56. B As tabelas globais do DynamoDB são um banco de dados multirregional e multiativo gerenciado, com replicação assíncrona automática e resolução de conflitos pela regra 'a última gravação vence' (last-writer-wins), com leituras e gravações de baixa latência em cada região. O RDS Multi-AZ dá alta disponibilidade só dentro de uma região. As réplicas de leitura do RDS só permitem gravar em uma região e exigem promoção manual para gravar. O ElastiCache for Redis em modo cluster é um cache em memória dentro de uma região, não durável nem multirregional.

57. D O backup e restauração (backup and restore) é a estratégia de recuperação de desastres de menor custo: guarda backups (por exemplo, no Amazon S3 ou pelo AWS Backup) e só reconstrói a infraestrutura quando o desastre ocorre. Recuperar em 24 horas e fazer backups periódicos (por exemplo, diários) atende com folga a um RTO e um RPO de 24 horas, com custo contínuo mínimo. A luz piloto, a espera morna e o multi-site ativo-ativo mantêm infraestrutura ligada, total ou parcial, em uma segunda região, com custo recorrente desnecessário para metas tão folgadas.

58. B A espera morna mantém em execução contínua, em uma região secundária, uma réplica reduzida e totalmente funcional da produção; em um desastre, ela é escalada para a carga total, com RTO menor que o da luz piloto e custo contínuo maior. A luz piloto mantém ligada só a infraestrutura essencial, como bancos replicados, e o resto precisa ser iniciado. O backup e restauração tem o maior RTO/RPO. O multi-site ativo-ativo atende a produção de várias regiões ao mesmo tempo.

59. B O RDS Multi-AZ replica os dados de forma síncrona para um standby em outra AZ e faz o failover automático (em geral de 60 a 120 segundos) se a AZ primária falhar, o que atende ao requisito de disponibilidade. Os snapshots diários só protegem contra perda de dados, não contra falha de AZ, e a restauração é demorada. Uma réplica de leitura na mesma AZ não dá redundância em nível de AZ. O RDS Single-AZ atrás de um balanceador continua com um ponto único de falha no banco, pois os balanceadores distribuem tráfego da aplicação, não fazem failover de banco.

60. A As tabelas globais do DynamoDB resolvem gravações simultâneas no mesmo item de forma automática, pela regra 'a última gravação vence', com base em horários internos de gravação, sem intervenção da aplicação. A ConditionalCheckFailedException só ocorre quando a aplicação usa gravações condicionais de forma explícita, não por conflitos da replicação entre regiões. O DynamoDB não usa relógios vetoriais nem mescla atributos. Não existe mecanismo embutido que pause a replicação à espera de resolução manual por Lambda.

61. B A espera morna mantém em execução contínua, na região de recuperação, uma réplica reduzida e funcional de cada camada, que escala para a carga total em minutos, o que atende a um RTO de 10 minutos e a um RPO baixo, sem o custo de uma capacidade total duplicada. O backup e restauração costuma ter RTO de horas. A luz piloto mantém só os dados centrais, e a computação precisa ser provisionada durante o evento, o que costuma passar de 10 minutos. O multi-site ativo-ativo atenderia, mas com um custo que a restrição exclui.

62. C As tabelas globais do DynamoDB oferecem replicação multirregional e multiativa totalmente gerenciada: cada região lê e grava localmente, com baixa latência, e as mudanças se propagam às outras. Um índice secundário global só adiciona padrões de consulta alternativos em uma única tabela e região. O RDS Multi-AZ com réplicas entre regiões aceita uma única região primária gravável, sem gravações multiativas. O ElastiCache for Redis em modo cluster escala dentro de uma região e não oferece replicação multiativa entre regiões.

63. C O ElastiCache for Redis com Multi-AZ e pelo menos uma réplica faz failover automático: detecta a falha do nó primário, promove uma réplica e atualiza o DNS do endpoint primário, sem reconfigurar a aplicação. Os clientes precisam se reconectar e repetir requisições que falharam. O Memcached não promove réplicas, e o Auto Discovery só ajuda a achar nós. Um Redis sem réplica não tem para quem promover, e o failover Multi-AZ não pode ser ativado sem réplica.

64. D O Aurora Global Database usa replicação dedicada baseada em armazenamento, com atraso típico abaixo de um segundo, e se recupera de uma interrupção regional ao promover uma região secundária, em geral em menos de um minuto; são valores típicos, não garantidos. Uma réplica de leitura do RDS entre regiões usa replicação assíncrona, com atraso que pode chegar a segundos ou minutos, e exige promoção. O DMS adiciona complexidade e não tem esses recursos. Restaurar backups replicados leva bem mais tempo.

65. C Uma zona de disponibilidade é um ou mais data centers distintos, com energia, rede e conectividade redundantes, em instalações separadas e isolados das falhas de outras AZs da mesma região. As regiões contêm várias AZs, e não o contrário, então 'coleção de regiões' está invertido. Um único rack é pequeno demais e não é como a AWS define os limites de resiliência. Os buckets do S3 são um serviço de armazenamento, não a definição de AZ. Entender essa hierarquia (região, AZ, data center) é a base de todo desenho de resiliência Multi-AZ na prova.

66. C O Amazon EFS é um sistema de arquivos NFS elástico e gerenciado que aceita leitura e gravação simultâneas de milhares de instâncias EC2 em várias zonas, quando há destinos de montagem (mount targets) em cada AZ, o que o torna ideal para cargas compartilhadas multi-AZ. O EBS Multi-Attach se limita a uma AZ e a volumes io1/io2 com sistemas de arquivos que reconhecem clusters. O S3 é armazenamento de objetos, não um sistema de arquivos POSIX compartilhado. O Instance Store é efêmero e local a uma instância.

67. D Em tabelas globais com consistência eventual multirregional, o DynamoDB aplica a regra 'a última gravação vence' com base em horários internos, então gravações simultâneas no mesmo item em regiões diferentes podem se sobrescrever em silêncio. Definir a região responsável pelas gravações pode evitar esses conflitos, e as gravações condicionais avaliam só a réplica local. O DynamoDB não rejeita gravações conflitantes com exceção, não usa relógio vetorial e não exige resolução manual: a replicação é automática.

68. A O cluster Multi-AZ do RDS (Multi-AZ DB cluster, para MySQL e PostgreSQL) oferece duas instâncias standby legíveis, com replicação semissíncrona e failover automático em geral abaixo de 35 segundos, o que permite transferir consultas de relatórios sem tocar na primária. O standby do Multi-AZ clássico não é legível. As réplicas de leitura replicam de forma assíncrona, com atraso maior, e não têm failover automático rápido. Os backups por snapshot não dão leitura em tempo real e servem à recuperação de desastres, não à alta disponibilidade.

69. A O RDS Multi-AZ replica os dados de forma síncrona para uma instância standby em outra AZ. Se a primária falha, o RDS inicia o failover automaticamente e muda o registro DNS CNAME para apontar para o standby, em geral em 60 a 120 segundos, sem necessidade de mudar o endpoint. O failover para réplica de leitura está errado, pois as réplicas são assíncronas e não fazem parte do failover automático Multi-AZ. Recriar na mesma AZ está errado, pois o failover vai para outra AZ. A promoção manual está errada, pois esse failover é totalmente automático.

Palavras-chave em inglês

Availability Zone (AZ)	zona de disponibilidade	Um ou mais data centers isolados dentro de uma região da AWS.

Region	região	Área geográfica da AWS com várias zonas de disponibilidade.
Multi-AZ	várias zonas de disponibilidade	Recursos em mais de uma zona para continuar se uma cair.
high availability	alta disponibilidade	O sistema fica no ar com o mínimo de interrupção.
fault-tolerant	tolerante a falhas	Continua funcionando mesmo quando um componente falha.
failover	failover, passagem para o recurso reserva	Passar o tráfego para outro recurso quando o principal falha.
disaster recovery	recuperação de desastres	Plano para restaurar o sistema depois de uma falha grave.
recovery time objective (RTO)	objetivo de tempo de recuperação	Tempo máximo aceitável para o sistema voltar a funcionar.
recovery point objective (RPO)	objetivo de ponto de recuperação	Máximo de dados recentes, medido em tempo, que se aceita perder.
decoupling	desacoplamento	Separar componentes para que um não dependa diretamente do outro.
queue	fila	Guarda mensagens até que outro componente as processe, como no SQS.
load balancer	balanceador de carga	Distribui o tráfego entre vários servidores.
target group	grupo de destino	Conjunto de recursos para onde o balanceador envia o tráfego.
health check	verificação de integridade	Teste periódico que mostra se uma instância está respondendo bem.
Auto Scaling	ajuste automático de escala	Aumenta ou diminui a quantidade de recursos conforme a demanda.
scalability	escalabilidade	Capacidade de crescer para atender a mais demanda.
operational overhead	sobrecarga operacional	Trabalho de administração e manutenção que a solução exige.
cost-effective	econômico	Que cumpre o que se pede gastando o mínimo possível.
workload	carga de trabalho	Aplicação ou processamento que roda na nuvem.
least privilege	privilégio mínimo	Dar só as permissões necessárias para a tarefa.
IAM role	função do IAM (também: perfil do IAM)	Identidade com permissões e credenciais temporárias que alguém assume.
IAM policy	política do IAM	Documento que permite ou nega ações em recursos da AWS.

trust policy	política de confiança	Define quem pode assumir uma função do IAM.
cross-account access	acesso entre contas	Permitir que uma conta AWS use recursos de outra conta.
confused deputy problem	problema do substituto confuso	Alguém sem permissão engana quem tem e faz essa parte agir.
encryption at rest	criptografia em repouso	Proteger dados guardados em disco, banco ou armazenamento.
encryption in transit	criptografia em trânsito	Proteger dados enquanto passam pela rede.
secrets management	gerenciamento de segredos	Guardar e trocar senhas e chaves sem escrevê-las no código.
Virtual Private Cloud (VPC)	nuvem privada virtual	Rede isolada que você configura dentro da AWS.
subnet	sub-rede	Faixa de endereços IP dentro da VPC.
security group	grupo de segurança	Firewall virtual que controla o tráfego de um recurso na VPC.
VPC endpoint	endpoint da VPC	Acesso privado a serviços da AWS sem passar pela internet pública.
storage class	classe de armazenamento	Categoria do S3 conforme frequência de acesso, custo e disponibilidade.
lifecycle policy	política de ciclo de vida	Regra que move ou apaga objetos automaticamente.
access pattern	padrão de acesso	Com que frequência e de que forma os dados são lidos ou gravados.
Spot Instances	instâncias Spot	Capacidade mais barata que a AWS pode interromper.
Reserved Instances	instâncias reservadas	Desconto em troca de compromisso de uso de um a três anos.
right-sizing	dimensionamento correto	Escolher recursos do tamanho de que a carga precisa.
caching	armazenamento em cache	Guardar cópias temporárias para responder mais rápido.
latency	latência	Tempo entre o pedido e a resposta.
warm standby	espera morna	Cópia reduzida e funcional do ambiente, pronta para escalar em um desastre.
pilot light	luz piloto	Só os serviços centrais ficam ligados na região de recuperação.
permissions boundary	limite de permissões	Define o máximo de permissões que uma entidade do IAM pode ter.
envelope encryption	criptografia de envelope	Uma chave de dados criptografa o objeto e o KMS protege essa chave.
global tables	tabelas globais	Replicação multirregional e multiativa do DynamoDB.

Origin Shield	Origin Shield	Camada extra de cache do CloudFront que reduz a carga na origem.
Intelligent-Tiering	Intelligent-Tiering	Classe do S3 que move objetos entre camadas conforme o acesso.
service control policy (SCP)	política de controle de serviço	Limita as permissões de contas ou OUs no AWS Organizations.

O Examundo é independente. Não é afiliado às entidades que fazem essas provas nem tem a aprovação delas. As questões são originais, não são da prova real. examundo.tech/pt/aws-solutions-architect-associate/