Strecht Simulados · Guia de preparação



Guia de preparação CLF-C02

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

4 capítulos por domínio	**28** questões comentadas	**70%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso CLF-C02: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 70%).

Mapa do exame

Cada prova do curso tem 65 questões e 90 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Domínio 1: Conceitos da nuvem	24%	18 conceitos · 14 pegadinhas
2. Domínio 2: Segurança e conformidade	30%	18 conceitos · 14 pegadinhas
3. Domínio 3: Tecnologia e serviços da nuvem	34%	18 conceitos · 14 pegadinhas
4. Domínio 4: Cobrança, preços e suporte	12%	15 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Domínio 1: Conceitos da nuvem

Uma empresa mantém um cluster MySQL em instâncias Amazon EC2, e dois administradores gastam boa parte da semana aplicando patches, configurando backups e testando a recuperação. Ao avaliar a migração para o Amazon RDS, qual redução de custo o serviço gerenciado traz que não aparece quando se compara só o preço por hora das instâncias?

A. Preço por hora da instância de banco menor que o da instância EC2 equivalente
B. Licença do MySQL Enterprise incluída no preço da instância de banco
C. Armazenamento incluído no preço da instância, sem cobrança por GB
D. Menos horas da equipe em tarefas operacionais como patches e backups

D2 · Domínio 1: Conceitos da nuvem

Em qual cenário faz mais sentido adotar o modelo de cobrança pay-as-you-go (pague conforme o uso) da AWS em vez de adquirir infraestrutura de TI tradicional on-premises?

A. Quando a empresa precisa de um investimento inicial elevado para depreciar servidores ao longo de vários anos
B. Quando a demanda de recursos de TI é altamente variável e imprevisível ao longo do tempo
C. Quando a organização não pretende alterar sua capacidade de computação pelos próximos 5 a 10 anos
D. Quando a principal exigência é manter a propriedade física dos próprios servidores e storages

D3 · Domínio 1: Conceitos da nuvem

Uma produtora tem 300 TB de vídeos num servidor de arquivos NFS no data center e quer levá-los para o Amazon S3 pela rede, com transferências agendadas, cópia só do que mudou desde a última execução e verificação de integridade dos dados. Qual serviço atende?

A. Amazon S3 Transfer Acceleration, com envio dos arquivos pelas edge locations
B. AWS DataSync, com agente no ambiente local e tarefas agendadas de transferência
C. AWS Storage Gateway com File Gateway, para que os servidores gravem num compartilhamento ligado ao S3
D. AWS Snowball Edge, com dispositivos físicos enviados ao data center para carga offline

D4 · Domínio 2: Segurança e conformidade

Uma empresa criptografa volumes Amazon EBS com a chave aws/ebs criada automaticamente na conta. A auditoria agora exige que a própria empresa defina quem pode usar a chave na política de chave, possa desabilitá-la quando necessário e escolha o período de rotação automática. O que ela deve usar?

A. Chave de propriedade da AWS (AWS owned key), usada pelo serviço sem custo para o cliente
B. Chave gerenciada pelo cliente no AWS KMS, com política de chave e rotação definidas pela empresa
C. A mesma chave gerenciada pela AWS, editando a política de chave aws/ebs para restringir o uso
D. Criptografia no sistema operacional da instância, com as chaves guardadas num arquivo do próprio volume

D5 · Domínio 2: Segurança e conformidade

Uma empresa global usa várias contas AWS em uma organização do AWS Organizations. A equipe de segurança quer garantir que nenhuma conta possa desativar o AWS CloudTrail nem modificar as trilhas de auditoria centralizadas, mesmo que usuários tenham permissões administrativas nas contas-membro. Qual é a abordagem MAIS adequada para atender a esse requisito de segurança?

A. Criar uma trilha em cada conta e usar políticas do IAM para negar a modificação das trilhas
B. Habilitar o AWS Config nas contas com regra que verifica se o CloudTrail está ativo e alerta
C. Definir um StackSet do CloudFormation com o CloudTrail e bloquear as atualizações do StackSet
D. Usar trilha da organização com logs em conta central e SCP que impede alterar o CloudTrail

D6 · Domínio 2: Segurança e conformidade

Uma aplicação em uma instância EC2 precisa ler objetos de um bucket do Amazon S3. Qual é a forma mais segura de conceder essa permissão?

A. Anexar uma função (role) do IAM à instância
B. Gravar chaves de acesso de um usuário IAM no código
C. Guardar chaves de acesso de um usuário IAM no Secrets Manager e lê-las na inicialização
D. Criar uma bucket policy que permita o IP público da instância

D7 · Domínio 3: Tecnologia e serviços da nuvem

Um grupo de segurança foi criado para uma instância EC2 e nenhuma regra de entrada foi adicionada. Como ele trata o tráfego por padrão?

A. Permite a entrada e a saída
B. Permite a entrada e bloqueia a saída
C. Bloqueia a entrada e a saída
D. Bloqueia a entrada e permite a saída

D8 · Domínio 3: Tecnologia e serviços da nuvem

Uma empresa está modernizando sua arquitetura na AWS e quer desacoplar componentes de uma aplicação para aumentar a resiliência e a escalabilidade. A empresa precisa de um serviço totalmente gerenciado que permita enviar, armazenar e processar mensagens de forma assíncrona entre diferentes microsserviços, garantindo que nenhuma mensagem seja perdida quando um consumidor estiver temporariamente indisponível. Qual serviço da AWS atende melhor a esse requisito?

A. AWS Step Functions
B. Amazon SQS
C. Amazon EventBridge
D. Amazon SNS

D9 · Domínio 3: Tecnologia e serviços da nuvem

Uma rede de varejo grava as vendas num banco relacional transacional. A área de inteligência quer rodar consultas analíticas complexas, com agregações sobre cinco anos de histórico que somam vários terabytes, sem prejudicar o desempenho do sistema de vendas. Qual serviço é indicado para essas análises?

A. Amazon DynamoDB com índices secundários globais para cada tipo de relatório
B. Amazon ElastiCache para manter em memória os resultados das consultas analíticas feitas anteriormente
C. Amazon RDS for MySQL com mais uma réplica de leitura dedicada às consultas
D. Amazon Redshift, um data warehouse com armazenamento colunar e processamento paralelo

D10 · Domínio 4: Cobrança, preços e suporte

Uma empresa está avaliando como otimizar custos em sua conta AWS e deseja identificar rapidamente quais serviços e recursos estão gerando a maior parte das despesas mensais, com possibilidade de detalhamento por conta vinculada, tag e região. Qual serviço ou ferramenta da AWS é MAIS adequado para essa análise detalhada de custos?

A. Consolidated Billing no AWS Organizations
B. AWS Cost Explorer
C. AWS Budgets
D. AWS Pricing Calculator

D11 · Domínio 4: Cobrança, preços e suporte

Uma empresa reuniu as contas de produção, desenvolvimento e dados numa organização do AWS Organizations com faturamento consolidado. O financeiro quer saber quem é responsável por pagar os custos gerados pelas contas-membro. Qual afirmação está correta?

A. A conta de administrador delegado escolhida pela empresa paga os custos das contas-membro
B. A conta que comprou as Instâncias Reservadas e os Savings Plans paga a fatura da organização
C. A conta de gerenciamento paga as cobranças geradas pelas contas-membro, numa fatura consolidada
D. Cada conta-membro continua pagando a própria fatura, e a organização só consolida os relatórios de custo

D12 · Domínio 4: Cobrança, preços e suporte

Uma empresa adotou AWS Organizations com consolidação de cobrança e deseja otimizar custos usando Savings Plans e Reserved Instances. O time financeiro quer receber uma visão centralizada de como esses descontos estão sendo aplicados entre as contas-membro, sem dar acesso administrativo total às contas. Qual combinação de ferramentas/recursos da AWS é a MAIS adequada para atender a esse requisito?

A. Configurar AWS Budgets individualmente em cada conta-membro e usar alertas de e-mail para inferir a distribuição de Savings Plans e Reserved Instances
B. Usar o AWS Trusted Advisor na conta de gerenciamento com a verificação de otimização de instâncias reservadas
C. Usar o Cost Explorer na conta de gerenciamento com os relatórios de utilização e cobertura de RIs e Savings Plans
D. Usar o AWS Cost Anomaly Detection na conta de gerenciamento

01

CAPÍTULO 1 · 24% DA PROVA

Domínio 1: Conceitos da nuvem

Aqui eu preciso dominar o 'porquê' da nuvem: as seis vantagens, os seis pilares do Well-Architected com seus princípios de design, as seis perspectivas e as quatro fases do AWS CAF, os 7 Rs de migração com as ferramentas certas e a economia da nuvem (CapEx x OpEx, TCO, BYOL x License Included). Vale 24% da nota e quase sempre vem como 'a empresa fez tal coisa: qual vantagem, pilar, princípio ou estratégia é essa?'. Onde eu mais erro: trocar princípios parecidos entre pilares (game day, rastreabilidade, recuperação automática), confundir elasticidade com escalabilidade, misturar rehost, relocate, replatform e repurchase e achar que ir para o EC2 elimina patches e licenças.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Seis vantagens da nuvem

Trocar despesa de capital por despesa variável; beneficiar-se de economias de escala; parar de adivinhar a capacidade; aumentar velocidade e agilidade; parar de gastar dinheiro operando data centers; tornar-se global em minutos. Cada uma responde a um problema típico: comprar para o pico (adivinhar capacidade), atender outro país rápido (global), não querer cuidar de racks e energia (data centers). Economia de escala só explica preço menor pelo uso agregado de muitos clientes.

Elasticidade e escalabilidade

Elasticidade é aumentar e reduzir recursos automaticamente conforme a demanda oscila, por exemplo reduzir à noite e crescer de manhã. Escalabilidade é a capacidade de suportar uma carga que cresce de forma sustentada. Demanda imprevisível (mil ou um milhão de usuários) aponta para elasticidade somada ao pagamento pelo uso.

Alta disponibilidade, tolerância a falhas e recuperação de desastres

Alta disponibilidade mantém a aplicação operando apesar de falhas de componentes ou de uma zona de disponibilidade, aceitando interrupção curta. Tolerância a falhas exige zero interrupção, com redundância ativa. Recuperação de desastres é voltar a funcionar após um evento grave, normalmente com dados em outra Região.

CapEx, OpEx e custos fixos x variáveis

Comprar servidores é despesa de capital (CapEx), mesmo que depreciada mês a mês. Pagar pelo uso da nuvem é despesa operacional (OpEx) e variável. Na migração, aluguel do espaço, energia e depreciação de hardware viram custo variável; salários de desenvolvimento e licenças por usuário continuam com a empresa.

TCO (custo total de propriedade)

Uma comparação justa soma, do lado on-premises, energia, refrigeração, espaço, rede, contratos de manutenção de hardware, horas da equipe de infraestrutura e a capacidade ociosa comprada para o pico. Ao ir para o EC2 somem os custos físicos; o sistema operacional convidado, os patches, as licenças e o código continuam sendo do cliente. Com serviço gerenciado (como RDS) somem também horas de patches e backups.

BYOL x License Included

BYOL reaproveita licenças já pagas; com Software Assurance e License Mobility vale em instâncias de locação padrão. Licenças por socket ou núcleo físico exigem Dedicated Hosts, que dão visibilidade de sockets e núcleos. Quem não tem licença paga a licença no preço por hora (License Included); sem querer administrar o SO, a opção é RDS com License Included.

AWS Well-Architected Framework

Seis pilares: Excelência Operacional, Segurança, Confiabilidade, Eficiência de Performance, Otimização de Custos e Sustentabilidade. A AWS Well-Architected Tool revisa uma carga contra os pilares e gera um plano de melhorias. Para cargas específicas (serverless, SaaS, ML) aplicam-se lentes oficiais do Lens Catalog; lentes personalizadas são escritas pelo próprio cliente.

Princípios do pilar Segurança

Implementar uma base de identidade forte (menor privilégio, separação de funções, sem credenciais de longo prazo); manter a rastreabilidade; aplicar segurança em todas as camadas; automatizar boas práticas (controles como código); proteger dados em trânsito e em repouso conforme a sensibilidade; manter as pessoas longe dos dados; preparar-se para eventos de segurança (simulações de incidente).

Princípios do pilar Confiabilidade

Recuperar automaticamente de falhas a partir de KPIs de negócio; testar os procedimentos de recuperação simulando falhas; escalar horizontalmente (vários recursos pequenos no lugar de um grande); parar de adivinhar a capacidade; gerenciar mudanças por meio de automação. Uma instância maior é escala vertical e mantém o ponto único de falha.

Princípios do pilar Excelência Operacional

Operações como código, observabilidade para insights acionáveis, mudanças frequentes, pequenas e reversíveis, refinar procedimentos com frequência, antecipar falhas (game days, pre-mortem), aprender com eventos operacionais (post-mortem sem culpados) e usar serviços gerenciados para reduzir a carga operacional.

Princípios do pilar Eficiência de Performance

Democratizar tecnologias avançadas (consumir como serviço o que exigiria especialistas), tornar-se global em minutos, usar arquiteturas serverless, experimentar com mais frequência (testes comparativos descartáveis) e considerar a afinidade mecânica (escolher banco ou armazenamento pelo padrão de acesso aos dados).

Princípios do pilar Otimização de Custos

Implementar a gestão financeira da nuvem (equipe, processos e cultura de custos); adotar um modelo de consumo (pagar pelo uso, desligar fora do expediente); medir a eficiência geral (resultado de negócio x custo); parar de gastar com trabalho pesado indiferenciado (serviços gerenciados); analisar e atribuir despesas a cada dono de carga.

Pilar Sustentabilidade

Tem modelo de responsabilidade compartilhada: sustentabilidade DA nuvem (data centers, energia renovável, refrigeração, água) é da AWS; sustentabilidade NA nuvem (dimensionar corretamente, remover ociosos, dados guardados) é do cliente. Princípios: entender o impacto, estabelecer metas, maximizar a utilização, antecipar e adotar ofertas de hardware e software mais eficientes, usar serviços gerenciados e reduzir o impacto downstream.

AWS CAF: perspectivas

Seis perspectivas. De negócio: Negócio (estratégia, portfólio, caso de negócio), Pessoas (cultura, capacitação, gestão da mudança) e Governança (programas, benefícios, riscos, finanças da nuvem). Técnicas: Plataforma (arquitetura, engenharia de dados, CI/CD), Segurança (identidade, detecção, proteção de dados, resposta a incidentes) e Operações (observabilidade, incidentes, capacidade).

AWS CAF: fases e benefícios

A jornada de transformação segue Envision, Align, Launch e Scale; pilotos em produção mostrando valor incremental = Launch. Os benefícios de negócio são redução de risco, melhor desempenho ESG, aumento de receita (novos produtos, clientes e mercados) e aumento da eficiência operacional.

Estratégias de migração (7 Rs)

Rehost (levar como está para o EC2), Replatform (pequenas otimizações, como trocar o banco por RDS), Refactor/Re-architect (reescrever para nativo da nuvem), Repurchase (trocar por SaaS), Relocate (VMware para a mesma plataforma na AWS), Retain (manter por enquanto) e Retire (desligar o que ninguém usa). Uma migração em grande escala passa pelas fases Assess, Mobilize e Migrate and modernize.

Ferramentas e programas de migração

Application Migration Service replica servidores para o EC2 (rehost). DMS migra bancos com carga completa + CDC; SCT converte esquema e código quando o mecanismo muda. DataSync move arquivos pela rede com agendamento e verificação. Para descoberta e ondas, cliente novo usa AWS Transform (Migration Hub e Application Discovery Service fechados a novos clientes); Migration Evaluator monta o caso de negócio; MAP oferece metodologia, parceiros e incentivos; Prescriptive Guidance traz padrões gratuitos.

Benefícios da infraestrutura global

Zonas de disponibilidade protegem contra a falha de um data center sem construir outro prédio. Regiões em vários continentes permitem copiar backups, AMIs e objetos do S3 para recuperar de um desastre regional e atender clientes distantes. Edge locations aproximam conteúdo em cache dos usuários sem implantar a aplicação em outras Regiões.

Macetes para memorizar

💡 Seis vantagens da nuvem

V-E-C-V-D-G: despesa Variável, Escala barateia, Capacidade sem chute, Velocidade e agilidade, Data center some, Global em minutos. Cada uma resolve um problema: pico, preço, país, prédio.

💡 Seis pilares do Well-Architected

SECOPS: Segurança, Excelência operacional, Confiabilidade, Otimização de custos, Performance e Sustentabilidade.

💡 Elasticidade x escalabilidade

Elástico estica e encolhe todo dia; escalável cresce ao longo do ano.

💡 Alta disponibilidade x tolerância a falhas

Alta disponibilidade pisca (minutos fora do ar); tolerância a falhas nem pisca (zero interrupção).

💡 7 Rs de migração

Mudança de casa: rehost leva os móveis como estão; replatform troca só o fogão; refactor reconstrói a casa; repurchase aluga mobiliado (SaaS); relocate leva o trailer inteiro (VMware); retain fica onde está; retire joga fora.

💡 AWS CAF

Negócio, Pessoas e Governança decidem; Plataforma constrói, Segurança protege, Operações mantém funcionando. Fases: Enxergar, Alinhar, Lançar, Escalar (Envision, Align, Launch, Scale).

Migração de bancos

Mesmo motor = DMS com carga completa + CDC. Motor diferente = SCT converte o esquema e o DMS move os dados.

Sustentabilidade

DA nuvem é da AWS (prédio, energia, água); NA nuvem é minha (tamanho certo, ociosos, dados guardados).

Tabela de memorização: não confunda

Quando é...	...e quando é
Elasticidade A demanda sobe e desce (dia x noite, picos imprevisíveis) e os recursos devem acompanhar automaticamente.	**Escalabilidade** A carga cresce de forma sustentada ao longo do tempo e o sistema precisa suportar mais.
Tolerância a falhas O sistema não pode ter nenhuma interrupção perceptível quando um componente falha.	**Alta disponibilidade** O sistema aceita alguns minutos de indisponibilidade enquanto o serviço é recuperado.
Rehost Servidores físicos ou virtuais vão para instâncias EC2 sem mudar SO e aplicação, com o Application Migration Service.	**Relocate** VMs VMware vão para a versão em nuvem da mesma plataforma, mantendo ferramentas e procedimentos da equipe.
Replatform A aplicação fica igual e ganha otimizações pontuais, como trocar o banco autogerenciado pelo RDS.	**Refactor** A aplicação é reescrita ou redesenhada para nativo da nuvem (microsserviços, Lambda, eventos).
Repurchase A função continua necessária, mas o sistema próprio é trocado por um produto comercial, em geral SaaS.	**Retire** O sistema não tem mais uso e é simplesmente desligado.
Excelência Operacional Operações como código, runbooks, game days para testar procedimentos e reação da equipe, lições aprendidas.	**Confiabilidade** A arquitetura se recupera sozinha de falhas, escala horizontalmente e tem a recuperação testada com falhas simuladas.
Migration Evaluator Caso de negócio da migração a partir do uso real medido no ambiente on-premises (coletor sem agente ou inventário exportado).	**AWS Pricing Calculator** Estimativa montada pela própria equipe, serviço a serviço, para uma arquitetura planejada.

Números que caem

Item	Valor
Peso do domínio na nota	**24%**

Pilares do Well-Architected / perspectivas do CAF / fases da jornada do CAF	**6 / 6 / 4**
Estratégias de migração / fases de uma migração em grande escala	**7 Rs / 3 (Assess, Mobilize, Migrate and modernize)**
Instâncias ligadas 50 das 168 horas da semana	**Economia de cerca de 70% em computação; EBS continua cobrado**
Snowball Edge e Application Discovery Service	**Fechados a novos clientes desde novembro de 2025**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que migrar para o EC2 elimina patches do sistema operacional e licenças por usuário.
Como não cair: No EC2 o SO convidado continua sendo do cliente. Saem apenas os custos físicos (energia, espaço, troca de discos e fontes); licenças e código continuam.

⚠ **Alerta de prova:** Responder 'economia de escala' para qualquer benefício financeiro ou de capacidade.
Como não cair: Economia de escala explica só o preço menor pelo uso agregado. Capacidade ociosa ou insuficiente é 'parar de adivinhar a capacidade'; chegar antes ao mercado é velocidade e agilidade (time to market).

⚠ **Alerta de prova:** Tratar Reserved Instances como servidores comprados, com prazo de cinco anos e depreciação no balanço.
Como não cair: RI é desconto de cobrança com prazo de 1 ou 3 anos. O hardware é sempre da AWS e o cliente troca de geração de instância quando quiser.

⚠ **Alerta de prova:** Usar Instâncias Reservadas ou o nível gratuito para um teste de duas semanas.
Como não cair: Experimentar barato e descartar o que falhar é a vantagem 'aumentar velocidade e agilidade': recursos sob demanda criados e excluídos ao fim do teste. O nível gratuito atual dá créditos limitados e RIs exigem compromisso de 1 ou 3 anos.

⚠ **Alerta de prova:** Trocar 'democratizar tecnologias avançadas' por 'parar de gastar com trabalho pesado indiferenciado' quando o cenário adota serviços gerenciados.
Como não cair: Se o motivo é não ter especialistas para hospedar ML, NoSQL ou mídia, é democratizar (Eficiência de Performance). Se é tirar a equipe da operação de servidores próprios (fila, e-mail) para focar no produto, é trabalho pesado indiferenciado (Otimização de Custos).

⚠ **Alerta de prova:** Escolher Application Discovery Service, Migration Hub ou Snowball Edge para um cliente novo.
Como não cair: Esses serviços não aceitam novos clientes. Descoberta e ondas de migração ficam com o AWS Transform; transferência de arquivos pela rede com agendamento, com o DataSync.

⚠ **Alerta de prova:** Usar o AWS Schema Conversion Tool numa migração de mesmo mecanismo (Oracle para RDS for Oracle, MySQL para RDS for MySQL).
Como não cair: SCT só entra quando o mecanismo muda (Oracle para Aurora PostgreSQL). Origem no ar e corte curto pedem DMS com carga completa + CDC.

⚠ **Alerta de prova:** Achar que parar instâncias fora do expediente também zera o custo dos volumes EBS.
Como não cair: Instância parada não cobra computação, mas o EBS é cobrado enquanto existir. Ligadas 50 de 168 horas, a economia em computação é de cerca de 70%, não 30%.

⚠ **Alerta de prova:** Acreditar que hospedar na AWS transfere a conformidade da aplicação e dos dados.
Como não cair: O cliente herda apenas os controles da infraestrutura certificada pela AWS; a conformidade do que ele coloca na nuvem continua sendo dele.

⚠ **Alerta de prova:** Usar Dedicated Instances para BYOL que exige saber sockets e núcleos físicos.
Como não cair: Dedicated Instances só isolam o hardware. Visibilidade de sockets e núcleos e afinidade com o mesmo servidor físico = Dedicated Hosts.

⚠ **Alerta de prova:** Colocar a energia renovável e a refrigeração dos data centers como ação de sustentabilidade do cliente.
Como não cair: Isso é sustentabilidade DA nuvem, papel da AWS. Ao cliente cabem dimensionamento correto, remoção de ociosos e maximização da utilização.

⚠ **Alerta de prova:** Responder 'Align' para a fase em que a empresa monta landing zone e prepara equipes antes de migrar em ondas.
Como não cair: Align é fase da jornada do AWS CAF. Nas três fases de migração em grande escala, preparar a organização é Mobilize.

⚠ **Alerta de prova:** Marcar 'preparar-se para eventos de segurança' quando o cenário é game day de procedimentos operacionais.
Como não cair: Game day de incidente de segurança = pilar Segurança. Procedimentos operacionais como código testados com a equipe = Excelência Operacional. Falhas simuladas para validar a recuperação da arquitetura = Confiabilidade.

⚠ **Alerta de prova:** Usar Local Zones ou edge locations do CloudFront como local de recuperação contra um desastre que derrube a Região.
Como não cair: Local Zones continuam ligadas à Região de origem e edge locations só fazem cache. Proteção regional = copiar backups, AMIs e objetos do S3 para outra Região; AZs protegem só dentro da Região.

Como cai na prova

📝 **Como cai:** A empresa adotou uma prática (simulações, painéis, templates versionados, várias instâncias pequenas) e pergunta qual princípio de design de um pilar ela aplica.
Como resolver: Ache o verbo da ação: simular falha da arquitetura = testar recuperação; KPI + automação = recuperar automaticamente; templates e pipelines = gerenciar mudanças por automação; game day de incidente de segurança = preparar-se para eventos de segurança. Descarte os princípios que pertencem a outro pilar.

📝 **Como cai:** Problema do data center próprio (servidores para o pico, preço alto, clientes em outro país, cuidar de racks) e a pergunta 'qual vantagem da nuvem resolve?'.
Como resolver: Mapeie o problema para a vantagem: pico = parar de adivinhar a capacidade; preço por uso agregado = economia de escala; outro país = global em minutos; racks e energia = parar de gastar com data centers; testar e descartar barato = velocidade e agilidade.

📝 **Como cai:** Descrição de um ou dois sistemas e a pergunta 'qual estratégia de migração se aplica?', às vezes com Escolha DUAS.
Como resolver: Faça quatro perguntas: o código muda (refactor)? o produto é trocado por SaaS (repurchase)? sai do VMware para o VMware na AWS (relocate)? ainda não dá para migrar ou ninguém usa (retain ou retire)? Se nada muda e vai para o EC2, é rehost; se só troca o banco por gerenciado, replatform.

📝 **Como cai:** Comparação de custos entre o data center e a AWS: qual custo ficou de fora do TCO ou qual deixa de existir ao migrar.
Como resolver: Separe custos físicos (energia, refrigeração, espaço, manutenção de hardware, equipe de infraestrutura), que somem ou viram variáveis, dos que continuam com a empresa (licenças por usuário, salários de desenvolvimento, SO convidado no EC2). Treinamento e gestão da mudança são investimentos pontuais da migração, não custo que passa a variar com o uso.

📝 **Como cai:** Uma etapa da migração e a pergunta 'qual serviço ou programa da AWS atende?'.
Como resolver: Descobrir inventário e ondas = AWS Transform; caso de negócio pelo uso real = Migration Evaluator; replicar servidores = Application Migration Service; banco = DMS (e SCT se o motor muda); arquivos pela rede = DataSync; metodologia, parceiros e incentivo = MAP; receitas gratuitas = Prescriptive Guidance.

📝 **Como cai:** Lista de capacidades (riscos, portfólio, CI/CD, incidentes, capacitação) e a pergunta 'qual perspectiva do AWS CAF?'.
Como resolver: Riscos, benefícios e finanças da nuvem = Governança; estratégia, portfólio e caso de negócio = Negócio; cultura e treinamento = Pessoas; arquitetura, dados e CI/CD = Plataforma; identidade e ameaças = Segurança; observabilidade, incidentes e capacidade = Operações.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Comprava servidores para o pico e ficava com capacidade ociosa ou faltando	**Parar de adivinhar a capacidade**
Uso agregado de centenas de milhares de clientes reduz o preço	**Economias de escala**
Atender clientes de outro país em poucos dias, sem data center no exterior	**Tornar-se global em minutos (Região próxima)**
Sem especialistas em ML, NoSQL ou mídia, a empresa consome a tecnologia como serviço em vez de formar equipe para hospedá-la	**Democratizar tecnologias avançadas (Eficiência de Performance)**
Escolher o banco pela forma como os dados são lidos e gravados	**Afinidade mecânica (mechanical sympathy)**
KPI de negócio piora e a automação substitui o componente sozinha	**Recuperar automaticamente de falhas (Confiabilidade)**
Implantações pequenas, várias por semana, fáceis de desfazer	**Mudanças frequentes, pequenas e reversíveis (Excelência Operacional)**
Trocar sistemas autogerenciados por serviços gerenciados para a equipe focar no produto	**Parar de gastar com trabalho pesado indiferenciado (Otimização de Custos)**
Guia em seis perspectivas: negócios, pessoas, governança, plataforma, segurança e operações	**AWS Cloud Adoption Framework**
Substituir o sistema próprio por um produto SaaS de mercado	**Repurchase**
Programa com metodologia em fases, parceiros e incentivo financeiro para migrar	**AWS Migration Acceleration Program (MAP)**
Receitas passo a passo de migração revisadas pela AWS, sem contratar consultoria	**AWS Prescriptive Guidance**
Criar ambiente de teste em minutos e excluí-lo se a ideia falhar, sem hardware parado	**Aumentar velocidade e agilidade (recursos sob demanda)**
Dois projetos-piloto em produção mostrando valor incremental antes de expandir	**Fase Launch do AWS CAF**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Economia de escala só explica preço menor; capacidade ociosa ou insuficiente é 'parar de adivinhar a capacidade'.
- Game day de procedimentos operacionais = Excelência Operacional; falha simulada para validar a recuperação = Confiabilidade; simulação de incidente de segurança = Segurança.
- Rehost leva ao EC2 sem mudar nada; relocate mantém VMware; replatform só troca peças (banco gerenciado); refactor reescreve.
- No EC2 o SO convidado, as licenças e o código continuam meus; somem só os custos físicos.
- Cliente novo: AWS Transform para descoberta e ondas, DataSync para arquivos pela rede; Migration Hub, Application Discovery Service e Snowball Edge não aceitam novos clientes.

Essenciais para a prova (checklist)

☐ Sei associar cada uma das seis vantagens da nuvem ao problema que ela resolve.

☐ Sei diferenciar elasticidade de escalabilidade e alta disponibilidade de tolerância a falhas e de recuperação de desastres.

☐ Sei citar os seis pilares do Well-Architected e reconhecer pelo menos três princípios de design de cada um.

☐ Sei separar as perspectivas de negócio (Negócio, Pessoas, Governança) das técnicas (Plataforma, Segurança, Operações) do AWS CAF e a ordem Envision, Align, Launch, Scale.

☐ Sei escolher entre rehost, replatform, refactor, repurchase, relocate, retain e retire a partir de um cenário.

☐ Sei qual ferramenta usar para replicar servidores, migrar bancos homogêneos e heterogêneos, mover arquivos e montar o caso de negócio.

☐ Sei montar um TCO correto e dizer quais custos somem e quais continuam ao ir para o EC2 ou para um serviço gerenciado.

☐ Sei quando usar BYOL, License Included e Dedicated Hosts.

☐ Sei dividir a responsabilidade de sustentabilidade entre a AWS e o cliente.

Questões de revisão do capítulo

R1.1 · Domínio 1: Conceitos da nuvem

Um marketplace monitora o número de pedidos concluídos por minuto. Quando esse indicador cai abaixo do esperado, uma automação é disparada para notificar a equipe e substituir os componentes com problema, sem esperar intervenção humana. Qual princípio de design do pilar Confiabilidade do AWS Well-Architected Framework essa abordagem representa?

A. Recuperar automaticamente a carga após falhas, a partir de KPIs que medem o valor para o negócio
B. Parar de adivinhar a capacidade, ajustando os recursos à demanda monitorada
C. Testar os procedimentos de recuperação, simulando falhas para validar o plano antes de um incidente real
D. Escalar horizontalmente, trocando um recurso grande por vários recursos menores

R1.2 · Domínio 1: Conceitos da nuvem

Um portal de notícias roda numa única instância Amazon EC2 que já está no maior tamanho da família escolhida. Em dias de grande audiência a instância satura e, quando ela falha, o site inteiro sai do ar. Qual abordagem resolve os dois problemas, seguindo os princípios de confiabilidade da AWS?

A. Mover a instância para um Dedicated Host, garantindo que o servidor físico fique reservado ao portal
B. Distribuir a carga entre várias instâncias menores atrás de um Elastic Load Balancing, com Auto Scaling
C. Comprar uma Instância Reservada para o tamanho atual, garantindo capacidade reservada na zona de disponibilidade
D. Trocar a instância por uma de outra família com mais vCPUs e memória, mantendo um único servidor mais potente

R1.3 · Domínio 1: Conceitos da nuvem

Uma empresa mantém um sistema de folha de pagamento desenvolvido internamente, caro de manter e de atualizar a cada mudança na legislação. Na migração, ela decidiu abandoná-lo e contratar uma solução de folha oferecida como SaaS, levando os dados dos funcionários. Qual estratégia de migração é essa?

A. Retire, desligando o sistema por não ter mais valor para o negócio
B. Repurchase, trocando o sistema por um produto comercial, em geral SaaS
C. Refactor, reescrevendo o sistema com arquitetura nativa de nuvem e serverless
D. Replatform, levando o sistema para a nuvem com otimizações como banco gerenciado

R1.4 · Domínio 1: Conceitos da nuvem

No plano de adoção da nuvem de uma seguradora, um grupo ficou responsável por gestão de identidades e acessos, detecção de ameaças, gestão de vulnerabilidades, proteção de dados e resposta a incidentes. Segundo o AWS Cloud Adoption Framework (AWS CAF), essas capacidades pertencem a qual perspectiva?

A. Governança (Governance)
B. Operações (Operations)
C. Plataforma (Platform)
D. Segurança (Security)

Respostas comentadas

R1.1. A) Recuperar automaticamente a carga após falhas, a partir de KPIs que medem o valor para o negócio

Por quê: No princípio 'recuperar-se automaticamente de falhas', os KPIs devem medir o valor entregue ao negócio, e não aspectos técnicos da operação. Quando um limite é ultrapassado, a automação notifica, rastreia e executa processos de recuperação; com automação mais sofisticada, é possível até antecipar e corrigir falhas antes que ocorram.

✗ B) Incorreta. Parar de adivinhar a capacidade trata de evitar a saturação ajustando recursos à demanda; o gatilho do cenário é a queda de um indicador de negócio, não a falta de capacidade.

✗ C) Incorreta. Testar a recuperação significa provocar falhas de forma controlada para validar os procedimentos; o cenário descreve a reação automática a uma falha real detectada por um indicador.

✗ D) Incorreta. Escalar horizontalmente reduz o impacto de uma falha distribuindo a carga entre recursos menores, mas não descreve a detecção por KPI seguida de recuperação automática.

> **Dica de prova:** KPI de negócio + automação que reage sozinha = recuperar-se automaticamente de falhas. Simular falhas de propósito = testar procedimentos de recuperação.

R1.2. B) Distribuir a carga entre várias instâncias menores atrás de um Elastic Load Balancing, com Auto Scaling

Por quê: O pilar Confiabilidade do AWS Well-Architected recomenda escalar horizontalmente para aumentar a disponibilidade agregada: trocar um recurso grande por vários menores e distribuir as requisições para que não compartilhem um ponto comum de falha. Escalar verticalmente (instância maior) tem limite de tamanho e não remove o ponto único de falha.

✗ A) Incorreta. Um Dedicated Host atende a requisitos de licença ou de isolamento físico; o portal continuaria num único servidor sujeito a saturação e falha.

✗ C) Incorreta. A Instância Reservada zonal reserva capacidade e dá desconto, mas não aumenta a quantidade de servidores nem elimina o ponto único de falha.

✗ D) Incorreta. Escalar verticalmente pode aliviar a carga por um tempo, mas mantém um único ponto de falha e esbarra no limite de tamanho das instâncias.

> **Dica de prova:** Instância maior = vertical (scale up). Mais instâncias atrás de um load balancer = horizontal (scale out), que também melhora a disponibilidade.

R1.3. B) Repurchase, trocando o sistema por um produto comercial, em geral SaaS

Por quê: Entre as estratégias de migração (os 7 Rs), repurchase significa substituir a aplicação por um produto diferente, em geral oferecido como SaaS, com novo modelo de licenciamento. É comum para CRM, RH e folha de pagamento, em que soluções de mercado eliminam o custo de manter código próprio.

✗ A) Incorreta. Retire é desativar um sistema que não é mais necessário; aqui a função de folha continua, só que em outro produto.

✗ C) Incorreta. Refactor reescreve ou rearquiteta a aplicação própria; a empresa deixa de desenvolver o sistema.

✗ D) Incorreta. Replatform leva a mesma aplicação com pequenas otimizações; a empresa abandona a aplicação própria.

> **Dica de prova:** Troca por produto SaaS = repurchase. Desligar = retire. Mesma app com ajustes = replatform. Reescrever = refactor.

R1.4. D) Segurança (Security)

Por quê: O AWS CAF organiza as capacidades em seis perspectivas: Negócio, Pessoas e Governança (foco de negócio) e Plataforma, Segurança e Operações (foco técnico). A perspectiva Segurança ajuda a garantir confidencialidade, integridade e disponibilidade dos dados e cargas, com capacidades que vão da gestão de identidades à resposta a incidentes.

✗ A) Incorreta. A perspectiva Governança cuida de gestão de programas e benefícios, gestão de riscos, gestão financeira da nuvem e de dados, não de detecção de ameaças e resposta a incidentes de segurança.

✗ B) Incorreta. A perspectiva Operações trata de observabilidade, gestão de eventos, incidentes e problemas operacionais, mudanças e desempenho, não de identidades e proteção de dados.

✗ C) Incorreta. A perspectiva Plataforma trata de arquitetura da plataforma, provisionamento, engenharia de dados e CI/CD, não das capacidades de segurança citadas.

> **Dica de prova:** Identidade, detecção de ameaças, vulnerabilidades, proteção de dados e resposta a incidentes no CAF = perspectiva Segurança.

02

CAPÍTULO 2 · 30% DA PROVA

Domínio 2: Segurança e conformidade

Aqui eu preciso dominar quem faz o quê no modelo de responsabilidade compartilhada (e como isso muda entre EC2, RDS, Lambda, Fargate, S3 e DynamoDB), o IAM com usuário raiz, roles, políticas e SCPs, criptografia e segredos (KMS, CloudHSM, Secrets Manager, Parameter Store), auditoria (CloudTrail x Config) e o time de detecção e proteção (GuardDuty, Inspector, Macie, Detective, Security Hub CSPM, WAF, Shield). Vale 30% da nota e as quatro alternativas costumam ser serviços de segurança plausíveis. Onde eu mais erro: achar que SCP concede permissão, trocar CloudTrail por Config, misturar GuardDuty, Inspector e Macie e supor que serviço gerenciado tira de mim rede, identidade e dados.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Modelo de responsabilidade compartilhada

A AWS responde pela segurança DA nuvem: instalações, hardware, hipervisor, rede global e descarte seguro de mídias (NIST 800-88). O cliente responde pela segurança NA nuvem: dados, identidades, configurações, SO convidado no EC2, security groups e escolhas de criptografia. Controles herdados são físicos e ambientais; compartilhados são patches, configuração e treinamento; específicos do cliente são proteção de serviços e comunicações (zonas).

Responsabilidade por tipo de serviço

No EC2 o cliente cuida do SO convidado e dos patches, mesmo com AMI da Amazon. No RDS a AWS aplica patches no SO e no mecanismo; o cliente define usuários do banco, security groups, acesso público e criptografia. No Lambda o cliente cuida do código, da role de execução e dos dados; no Fargate, da imagem do contêiner e suas bibliotecas. Em DynamoDB e S3 a AWS cuida de servidores e replicação entre AZs.

Usuário raiz

Proteja com MFA (de preferência mais de um dispositivo), sem chaves de acesso, com e-mail de grupo da empresa e uso só para tarefas exclusivas. Exigem o raiz: alterar e-mail e senha do raiz, fechar a conta, restaurar o administrador IAM que se trancou e ativar o acesso do IAM ao Billing. Políticas do IAM não limitam o raiz; só uma SCP, quando a conta é membro de organização.

Identidades do IAM

Usuários IAM têm credenciais de longo prazo (senha e chaves de acesso). Grupos contêm só usuários, não se aninham e nunca são Principal de política de recurso. Roles são assumidas e entregam credenciais temporárias emitidas pelo AWS STS; aplicação em EC2 recebe permissão por role anexada, nunca por chave no código. Negação explícita sempre vence qualquer permissão.

Tipos de política

Política baseada em identidade fica no usuário, grupo ou role e não tem elemento Principal; política baseada em recurso (bucket policy) fica no recurso e indica quais principais acessam. Gerenciada pela AWS não pode ser editada; gerenciada pelo cliente é reutilizável e versionada; inline é um para um. Permissions boundary é o teto de permissões de roles criadas por um administrador delegado.

Service Control Policies e AWS Organizations

SCP define o máximo de permissões das contas de uma OU ou organização, inclusive para administradores das contas-membro, mas não concede nada. Serve para impedir ações como desativar o CloudTrail. Organizations com OUs e SCPs é a resposta para governança e limites por ambiente em várias contas.

IAM Identity Center e federação

Centraliza o acesso de usuários corporativos (AD, IdP SAML) a várias contas, sem criar usuários IAM em cada uma. Permission sets definem uma vez o acesso padronizado em dezenas de contas. Identidades do Identity Center e federadas assumem roles com credenciais temporárias; na CLI, aws sso login substitui chaves de longo prazo.

Acesso entre contas

A conta de destino cria uma role cuja trust policy confia na conta de origem, restringida com condições como aws:PrincipalOrgID. Compartilhar chaves de usuário IAM entre contas é má prática. Auditores ou consultores temporários recebem role com ReadOnlyAccess via federação, não usuários IAM.

Relatórios de credenciais e de acesso

Credential report é o CSV com status de senha, MFA e idade e uso das chaves de cada usuário IAM. Last accessed mostra quais serviços uma identidade realmente usou, para reduzir permissões. IAM Access Analyzer aponta buckets, roles e outros recursos compartilhados com contas externas ou com o público.

MFA e chaves de acesso

MFA é a resposta para senha vazada ou phishing; contra phishing de código de seis dígitos, a resposta é passkey ou chave de segurança FIDO, não outro gerador TOTP. Se uma chave de acesso precisar existir: usuário dedicado, menor privilégio, rotação e exclusão das sem uso. Chave exposta: a AWS avisa e pode aplicar política de quarentena; excluir a chave e investigar a conta é tarefa do cliente.

AWS KMS e AWS CloudHSM

KMS é gerenciado, multilocatário e integrado aos serviços, com trilha de auditoria. Chave gerenciada pela AWS (alias aws/serviço) não permite alterar a política, desabilitar nem mudar a rotação anual; chave gerenciada pelo cliente permite. CloudHSM entrega HSMs dedicados de locatário único, FIPS 140 nível 3, com usuários fora do IAM e APIs como PKCS #11.

Secrets Manager, Parameter Store e ACM

Secrets Manager guarda senhas e chaves de API com rotação automática nativa; com a integração do RDS, gerencia a senha mestre sem escrever função Lambda. Parameter Store guarda configurações hierárquicas e SecureString ao menor custo, sem rotação nativa. AWS Certificate Manager provisiona e renova certificados TLS para ALB e CloudFront.

Criptografia em repouso e em trânsito

Desde janeiro de 2023 o S3 aplica SSE-S3 a todo objeto novo; exigir chave do KMS pede criptografia padrão do bucket com SSE-KMS. No EBS, a criptografia por padrão precisa ser ativada em cada Região. Dados viajando pela rede pedem TLS/HTTPS (no CloudFront, política de protocolo do visualizador redirecionando HTTP para HTTPS). Criptografar antes de enviar com chave própria é criptografia do lado do cliente, responsabilidade do cliente.

AWS CloudTrail

Registra quem chamou qual API, quando e de onde, inclusive ações feitas no console. O Event history é ativo por padrão e mostra 90 dias de eventos de gerenciamento; retenção longa, eventos de dados (leitura de objetos do S3) e envio ao CloudWatch Logs exigem uma trilha. Auditoria robusta: trilha multirregião ou da organização, bucket com versionamento, Object Lock e validação de integridade, e SCP impedindo alterar o CloudTrail.

AWS Config

Mantém o histórico de configuração de cada recurso e avalia conformidade contínua com regras gerenciadas. Detecta e alerta, mas não impede ações. Conformance packs implantam várias regras de uma vez a partir de modelos (como PCI DSS); o agregador dá visão central de várias contas e Regiões; a remediação automática usa Systems Manager Automation.

Serviços de detecção

GuardDuty detecta ameaças ativas a partir de CloudTrail, VPC Flow Logs e DNS (credencial comprometida, mineração de criptomoedas), com Runtime Monitoring para contêineres e Malware Protection for S3. Inspector procura CVEs em EC2, imagens do ECR e Lambda e calcula alcançabilidade de rede. Macie descobre dados sensíveis no S3. Detective investiga a causa raiz com gráficos de comportamento. Security Hub CSPM agrega achados e confere padrões como CIS e FSBP.

Proteção de rede e de aplicação

Security group fica na instância, é stateful e só tem regras de permissão; um novo bloqueia entrada e libera saída. Network ACL fica na sub-rede, é stateless e aceita negação. AWS WAF bloqueia SQL injection, XSS e excesso de requisições por IP (regra rate-based) em CloudFront, ALB e API Gateway. Shield Standard é gratuito e automático; Shield Advanced traz equipe de resposta (SRT), proteção de custos e proteção de Elastic IPs e Global Accelerator. Firewall Manager aplica essas regras em toda a organização.

Onde achar informação de conformidade e segurança

AWS Artifact Reports entrega relatórios de auditoria da AWS (SOC, ISO, PCI); Artifact Agreements aceita acordos como o BAA da HIPAA, para a organização inteira pela conta de gerenciamento. AWS Services in Scope diz se um serviço está no escopo de um programa; páginas de programas de conformidade tratam de leis como LGPD. Security Bulletins avisam sobre vulnerabilidades, Security Blog traz novidades e boas práticas, Security Documentation orienta serviço por serviço. Pentest em serviços da lista dispensa aprovação prévia; DoS, DDoS e flooding são proibidos.

Macetes para memorizar

💡 Responsabilidade compartilhada

DA nuvem = AWS (o que eu não vejo nem toco: prédio, hardware, hipervisor). NA nuvem = eu (tudo que configuro no console ou na CLI: dados, IAM, security group, SO do EC2).

💡 SCP

SCP é teto, não escada: limita até o administrador, mas nunca concede nada.

💡 Trilha x configuração x métrica

CloudTrail = Trilha de quem fez; Config = Configuração de como estava; CloudWatch = Watch, olhar métricas, logs e alarmes.

💡 Detecção

GuardDuty é o Guarda vigiando ameaça agora; Inspector é o Inspetor de vulnerabilidade (CVE); Macie acha dados pessoais; Detective investiga a causa; Security Hub CSPM é o painel que junta tudo.

💡 Security group x network ACL

Security group só sabe dizer sim (allow) e lembra a resposta (stateful); NACL sabe dizer não (deny) e não lembra nada (stateless).

💡 Segredos

Secrets Manager rotaciona; Parameter Store só guarda (barato, hierárquico); KMS guarda chaves de criptografia, não senhas.

💡 Shield

Standard é de graça para todo mundo; Advanced é pago e traz SRT 24x7, proteção de custos e cobertura de Elastic IP e Global Accelerator.

💡 Usuário raiz e MFA

Raiz: MFA, zero chaves, e-mail de grupo e quase nunca usado. Phishing que rouba código de seis dígitos se vence com passkey ou chave FIDO, não com outro TOTP.

Tabela de memorização: não confunda

Quando é...	...e quando é
AWS CloudTrail Quem fez o quê, quando e de onde: chamadas de API, exclusão de bucket, logins, leitura de objetos (eventos de dados).	**AWS Config** Como cada recurso estava configurado ao longo do tempo e se está conforme as regras.
Amazon GuardDuty Ameaça acontecendo: tráfego para IP de mineração, credencial comprometida, processo suspeito em contêiner, malware enviado ao S3.	**Amazon Inspector** Vulnerabilidade de software conhecida (CVE) em EC2, ECR ou Lambda e portas alcançáveis pela configuração de rede.
Amazon GuardDuty Detectar a atividade maliciosa e gerar o achado.	**Amazon Detective** Investigar a causa raiz do achado com gráficos de relações e comportamento ao longo do tempo, sem escrever consultas.
Security group Liberar portas e origens na instância, com respostas liberadas automaticamente (stateful).	**Network ACL** Negar um IP ou intervalo específico para toda a sub-rede, com regras numeradas de permissão e negação (stateless).
AWS KMS Chaves gerenciadas, integradas aos serviços, com auditoria e rotação, sem manter hardware.	**AWS CloudHSM** HSM dedicado de locatário único, controle exclusivo, usuários fora do IAM e APIs como PKCS #11.
AWS Secrets Manager Senha de banco ou chave de API com rotação automática.	**Systems Manager Parameter Store** Configurações hierárquicas (/prod/app/), algumas como SecureString, sem rotação e ao menor custo.
Service Control Policy Limitar o que contas inteiras da organização podem fazer, até para administradores locais.	**Política do IAM / permissions boundary** Conceder permissões a uma identidade dentro da conta; o boundary limita só as roles criadas por um administrador delegado.

Números que caem

Item	Valor
Peso do domínio na nota	**30%**
Event history do CloudTrail	**90 dias de eventos de gerenciamento, ativo por padrão**
Criptografia SSE-S3 automática em objetos novos do S3	**Desde janeiro de 2023**
Rotação de chave gerenciada pela AWS no KMS	**Anual, sem o cliente poder alterar**
Validação dos HSMs do CloudHSM	**FIPS 140 nível 3**

Descarte de mídias pela AWS	**Técnicas do NIST 800-88**
Código TOTP de MFA	**Seis dígitos, renovado a cada 30 segundos no token de hardware**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar uma SCP para dar acesso de leitura a auditores ou a um time em várias contas.
Como não cair: SCP só limita, nunca concede. Acesso exige role ou permission set do IAM Identity Center.

⚠ **Alerta de prova:** Criar regra de negação no security group para bloquear um intervalo de IPs.
Como não cair: Security group só tem regras de permissão. Negar IP específico na sub-rede = network ACL; por taxa de requisições HTTP = WAF rate-based.

⚠ **Alerta de prova:** Escolher AWS Config para impedir que administradores desativem o CloudTrail.
Como não cair: Config detecta e alerta depois do fato. Impedir a ação, até para administradores, é SCP no AWS Organizations.

⚠ **Alerta de prova:** Manter as chaves do raiz e restringi-las com política do IAM, rotacioná-las ou guardá-las no Secrets Manager.
Como não cair: Políticas do IAM não limitam o raiz e chave guardada continua sendo credencial total de longo prazo. Exclua as chaves e use uma role com acesso mínimo.

⚠ **Alerta de prova:** Procurar no Event history do CloudTrail quem leu objetos de um bucket.
Como não cair: O Event history mostra só eventos de gerenciamento dos últimos 90 dias. Leituras de objetos exigem trilha com eventos de dados do S3.

⚠ **Alerta de prova:** Achar que, por ser serviço gerenciado, a AWS controla quem acessa a rede do RDS.
Como não cair: Acesso público, security groups e network ACLs do RDS são configurados pelo cliente; a AWS cuida de SO e mecanismo.

⚠ **Alerta de prova:** Esperar que o Amazon Inspector aplique as correções que encontrou.
Como não cair: Inspector encontra e prioriza vulnerabilidades. Aplicar patches em massa com baselines e janelas = Systems Manager Patch Manager.

⚠ **Alerta de prova:** Usar o Macie para verificar se um arquivo enviado ao S3 contém malware.
Como não cair: Macie acha dados sensíveis (CPF, cartão). Malware em objeto do S3 = GuardDuty Malware Protection for S3.

⚠ **Alerta de prova:** Aplicar S3 Object Lock no modo governança quando ninguém, nem o raiz, pode apagar.
Como não cair: No modo governança quem tem s3:BypassGovernanceRetention altera a retenção. Imutável para todos = modo compliance. MFA Delete também não basta.

⚠ **Alerta de prova:** Acreditar que a AWS tem 'certificação HIPAA' ou que baixar o relatório no Artifact formaliza o acordo.
Como não cair: Não existe certificação HIPAA. O BAA é aceito em Artifact Agreements e a PHI só pode ficar em serviços qualificados para HIPAA; criptografia não torna um serviço elegível.

⚠ **Alerta de prova:** Achar que o Shield Standard inclui equipe de resposta a DDoS e proteção de custos.
Como não cair: Standard é automático e gratuito. SRT 24x7, proteção de custos e proteção de Elastic IP e Global Accelerator exigem Shield Advanced.

⚠ **Alerta de prova:** Pensar que todo pentest precisa de aprovação prévia da AWS ou que o Shield Advanced libera simulação de DDoS.
Como não cair: Serviços da lista (como EC2, RDS, CloudFront e Lambda) podem ser testados sem aprovação; DoS, DDoS e flooding são proibidos pela política.

⚠ **Alerta de prova:** Usar o IAM Identity Center ou o AD Connector para servidores Windows ingressarem num domínio depois de fechar o data center.
Como não cair: Identity Center dá acesso às contas e aplicações da AWS, não um domínio AD, e o AD Connector só encaminha para um AD local existente. AD de verdade sem gerenciar controladores = AWS Managed Microsoft AD.

⚠ **Alerta de prova:** Aninhar grupos do IAM ou citar um grupo como Principal numa bucket policy.
Como não cair: Grupos contêm só usuários, não se aninham e não são entidade autenticada. Em política de recurso, cite usuário, role ou conta.

Como cai na prova

📝 **Como cai:** Lista de tarefas e a pergunta 'qual é responsabilidade da AWS (ou do cliente)?', às vezes citando o serviço usado.
Como resolver: Pergunte se a tarefa se configura no console, CLI ou API: se sim, é do cliente. Depois ajuste pelo serviço: no EC2 o SO é do cliente; no RDS, SO e mecanismo são da AWS, mas usuários do banco, security group e criptografia são do cliente; no Lambda e no Fargate, o cliente cuida de código, imagem e permissões.

📝 **Como cai:** Requisito de auditoria ('quem excluiu', 'histórico de configuração', 'conexões aceitas ou rejeitadas', 'ERROR nos logs') e quatro serviços de registro.
Como resolver: Chamada de API = CloudTrail (leitura de objeto exige trilha com eventos de dados); estado e conformidade dos recursos = Config; tráfego IP e porta = VPC Flow Logs; métricas e logs da aplicação com alarme = CloudWatch.

📝 **Como cai:** Achados de segurança variados e a pergunta 'qual serviço gerou ou atende cada um?'.
Como resolver: Ameaça ativa (IP malicioso, credencial comprometida, malware) = GuardDuty; CVE ou porta exposta = Inspector; CPF e cartões no S3 = Macie; causa raiz = Detective; painel e padrão CIS ou FSBP = Security Hub CSPM.

📝 **Como cai:** Requisito de bloquear algo em várias contas 'mesmo para administradores' ou de dar acesso a um time em muitas contas.
Como resolver: Bloquear = SCP no Organizations (ou Control Tower com controles preventivos e detectivos). Conceder = role ou permission set do IAM Identity Center. Lembre que SCP sozinha nunca dá acesso.

📝 **Como cai:** Aplicação, script ou pessoa precisa de credencial e a pergunta 'qual a forma mais segura?'.
Como resolver: Prefira sempre credencial temporária: role anexada ao EC2, role entre contas com trust policy restrita, IAM Identity Center com aws sso login. Chave de acesso só como exceção, com menor privilégio e rotação; chave no raiz, nunca.

📝 **Como cai:** Auditor pede documento ou informação de conformidade e a pergunta 'onde encontrar?'.
Como resolver: Relatório SOC, ISO ou PCI da AWS = Artifact Reports; BAA da HIPAA = Artifact Agreements; serviço está no escopo do programa = Services in Scope; lei de um país (LGPD) = páginas de programas de conformidade; aviso de vulnerabilidade = Security Bulletins.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Quem excluiu o recurso e em que horário a chamada foi feita	**AWS CloudTrail**
Histórico ou linha do tempo de configuração para conformidade	**AWS Config**
Impedir mesmo administradores das contas-membro	**Service Control Policies no AWS Organizations**
Relatórios SOC, ISO ou PCI da própria AWS para auditores	**AWS Artifact**

CPF, cartões ou dados pessoais em buckets do S3	**Amazon Macie**
CVE em instância EC2, imagem de contêiner ou função Lambda	**Amazon Inspector**
Credencial comprometida, IP de mineração, análise contínua de logs	**Amazon GuardDuty**
Painel único de achados e verificação contra CIS ou FSBP	**AWS Security Hub CSPM**
SQL injection, cross-site scripting ou limite de requisições por IP	**AWS WAF**
Milhões de clientes de aplicativo fazendo cadastro e login, inclusive com redes sociais	**Amazon Cognito**
Usuários do diretório corporativo acessando várias contas sem usuários IAM	**AWS IAM Identity Center**
Senha de banco fora do código com troca automática	**AWS Secrets Manager**
Triagem dos achados e engenheiros da AWS 24x7 para conter um incidente de segurança (não DDoS)	**AWS Security Incident Response (o Detective só apoia a investigação do próprio time; DDoS = Shield Advanced com SRT)**
Planilha com status de senha, MFA e idade das chaves de todos os usuários do IAM	**Credential report do IAM (serviços usados por uma identidade = last accessed)**

🎯 Se você lembrar de só uma coisa deste capítulo...

- SCP limita, nunca concede; negação explícita sempre vence.
- CloudTrail registra quem fez; Config registra como estava e avalia conformidade, mas não impede nada.
- Security group só tem allow; para negar IP, network ACL; para SQL injection, XSS e excesso de requisições, WAF.
- Usuário raiz: MFA, sem chaves de acesso, só para tarefas exclusivas; políticas do IAM não o limitam.
- Serviço gerenciado não transfere para a AWS dados, IAM, security groups e escolhas de criptografia.

Essenciais para a prova (checklist)

- ☐ Sei dividir entre AWS e cliente as responsabilidades em EC2, RDS, Lambda, Fargate, S3 e DynamoDB.
- ☐ Sei como proteger o usuário raiz e quais tarefas só ele executa.

☐ Sei diferenciar usuário, grupo, role, política de identidade, política de recurso, permissions boundary e SCP.

☐ Sei que negação explícita vence e que SCP não concede permissão.

☐ Sei quando usar KMS, CloudHSM, Secrets Manager, Parameter Store e Certificate Manager.

☐ Sei o que o S3 e o EBS criptografam por padrão e o que precisa ser configurado.

☐ Sei separar CloudTrail, Config, CloudWatch e VPC Flow Logs pelo tipo de evidência que cada um gera.

☐ Sei associar GuardDuty, Inspector, Macie, Detective e Security Hub CSPM ao achado correto.

☐ Sei quando usar security group, network ACL, WAF, Shield Standard, Shield Advanced e Firewall Manager.

☐ Sei onde encontrar relatórios, acordos, escopo de programas e avisos de segurança da AWS.

Questões de revisão do capítulo

R2.1 · Domínio 2: Segurança e conformidade

Um banco precisa, por exigência regulatória, guardar suas chaves criptográficas em HSMs dedicados de um único locatário, validados FIPS 140 nível 3, sob controle exclusivo da própria equipe, com gestão de usuários do HSM fora do IAM e uso de APIs padrão como PKCS #11. Qual serviço atende a esse requisito?

A. AWS CloudHSM, com um cluster de HSMs na VPC gerenciados pela equipe de segurança do banco
B. AWS KMS com chaves gerenciadas pelo cliente e política de chave restrita à equipe de segurança
C. AWS Secrets Manager, com rotação automática dos segredos que protegem as chaves do banco
D. AWS Certificate Manager, com certificados privados emitidos para as aplicações do banco

R2.2 · Domínio 2: Segurança e conformidade

Um portal de vagas recebe currículos enviados pelos candidatos e grava os arquivos num bucket do Amazon S3. A empresa quer que cada novo objeto seja verificado automaticamente contra malware antes de ser processado, com o resultado gravado como tag no próprio objeto. Qual recurso atende?

A. GuardDuty Malware Protection for S3 no bucket que recebe os uploads
B. Amazon Inspector com varredura de vulnerabilidades em pacotes de software
C. AWS Security Hub CSPM com o padrão Foundational Security Best Practices
D. Amazon Macie com descoberta automatizada de dados sensíveis no bucket

R2.3 · Domínio 2: Segurança e conformidade

Uma empresa ainda usa usuários do IAM para alguns acessos ao console, e a auditoria exige senhas com no mínimo 14 caracteres, letras maiúsculas, números e símbolos, expiração a cada 90 dias e bloqueio da reutilização das últimas cinco senhas. Como atender com o menor esforço?

A. Configurar a política de senha personalizada da conta nas configurações do IAM
B. Ativar a regra gerenciada iam-password-policy do AWS Config para avaliar a conta
C. Definir as regras de senha num grupo de usuários do Amazon Cognito ligado à conta
D. Criar uma política de controle de serviço (SCP) no AWS Organizations com as regras de senha

R2.4 · Domínio 2: Segurança e conformidade

Uma equipe de segurança precisa garantir que apenas workloads em uma conta específica da AWS consigam assumir uma role em outra conta da mesma organização. Qual abordagem é a MAIS adequada para restringir esse acesso entre contas, seguindo boas práticas de segurança e conformidade na AWS?

A. Criar um usuário IAM na conta de destino e compartilhar as chaves de acesso com a conta de origem, guardadas em um cofre de senhas
B. Usar uma SCP no AWS Organizations para negar o acesso de outras contas, dispensando a trust policy da role
C. Permitir na trust policy as contas da organização inteira e exigir MFA de quem assumir a role
D. Configurar a trust policy da role na conta de destino para confiar no ARN da conta de origem, com a condição aws:PrincipalOrgID

Respostas comentadas

R2.1. A) AWS CloudHSM, com um cluster de HSMs na VPC gerenciados pela equipe de segurança do banco

Por quê: AWS KMS e AWS CloudHSM protegem chaves em HSMs, mas com modelos diferentes. O KMS é gerenciado pela AWS e integrado aos serviços, com acesso controlado pelo IAM. O CloudHSM dá ao cliente um cluster de HSMs de locatário único, com controle total das chaves e dos usuários do HSM e APIs padrão, em troca de mais responsabilidade operacional.

✗ B) Incorreta. O AWS KMS é um serviço gerenciado e multilocatário, com permissões controladas pelo IAM e pelas políticas de chave; ele não entrega HSMs dedicados com gestão de usuários própria.

✗ C) Incorreta. O Secrets Manager guarda e rotaciona segredos como senhas e chaves de API; não fornece HSMs dedicados para gerar e usar chaves criptográficas.

✗ D) Incorreta. O ACM provisiona e renova certificados TLS; não atende à exigência de HSM dedicado sob controle do cliente.

> **Dica de prova:** HSM dedicado, locatário único, controle exclusivo e APIs como PKCS #11 = CloudHSM. Chaves gerenciadas e integradas aos serviços = KMS.

R2.2. A) GuardDuty Malware Protection for S3 no bucket que recebe os uploads

Por quê: O GuardDuty Malware Protection for S3 inicia uma verificação sempre que um objeto é enviado ao bucket protegido, publica o resultado no EventBridge e no CloudWatch e, se a marcação estiver ativada, grava uma tag com o resultado no objeto, o que permite bloquear o processamento de arquivos infectados. Pode ser usado junto com o GuardDuty ou como recurso independente.

✗ B) Incorreta. O Inspector procura vulnerabilidades conhecidas (CVEs) em EC2, imagens de contêiner e funções Lambda, não em arquivos enviados ao S3.

✗ C) Incorreta. O Security Hub CSPM confere controles de configuração e agrega achados de outros serviços; ele não verifica o conteúdo dos objetos.

✗ D) Incorreta. O Macie encontra dados sensíveis, como CPF e endereço nos currículos, mas não verifica se o arquivo contém malware.

> **Dica de prova:** Dado sensível ou pessoal no S3 = Macie. Arquivo malicioso enviado ao S3 = GuardDuty Malware Protection for S3.

R2.3. A) Configurar a política de senha personalizada da conta nas configurações do IAM

Por quê: A política de senha da conta vale para as senhas dos usuários do IAM, não para o usuário root nem para chaves de acesso. Sem política personalizada, vale a padrão (mínimo de 8 caracteres, três tipos de caracteres e sem expiração). A AWS recomenda combinar uma política de senha forte com MFA.

✗ B) Incorreta. A regra iam-password-policy do AWS Config avalia se a política de senha da conta atende aos parâmetros, mas não impõe as regras; a política ainda precisa ser configurada no IAM.

✗ C) Incorreta. Grupos de usuários do Cognito autenticam usuários de aplicações; suas regras de senha não valem para usuários do IAM que acessam o console.

✗ D) Incorreta. SCPs limitam as ações permitidas nas contas de uma organização; não definem requisitos de complexidade, expiração ou reutilização de senhas.

> **Dica de prova:** Comprimento, complexidade, expiração e reutilização de senhas dos usuários do IAM = política de senha da conta no IAM. Config só verifica; não impõe.

R2.4. D) Configurar a trust policy da role na conta de destino para confiar no ARN da conta de origem, com a condição aws:PrincipalOrgID

Por quê: No acesso entre contas, a role fica na conta de destino e sua trust policy define quem pode assumi-la. Confiar só no ARN da conta de origem aplica o menor privilégio, e a condição aws:PrincipalOrgID garante que o principal pertence à organização. A conta de origem concede a seus workloads permissão para chamar sts:AssumeRole, e as credenciais obtidas são temporárias.

✗ A) Incorreta. Compartilhar chaves de acesso de usuário IAM entre contas viola boas práticas de segurança, aumenta o risco de vazamento de credenciais e dificulta auditoria e rotação de chaves.

✗ B) Incorreta. SCPs limitam o que as contas podem fazer, mas não substituem a trust policy, que é o que define quem pode assumir a role.

✗ C) Incorreta. Confiar em todas as contas da organização amplia demais quem pode assumir a role; o MFA não corrige o escopo excessivo da trust policy e fere o menor privilégio.

> **Dica de prova:** Para acesso entre contas, pense sempre em: (1) usar roles IAM, não compartilhar chaves; (2) restringir a trust policy ao mínimo necessário (conta específica, organização, condições); (3) combinar com logs do AWS CloudTrail para auditoria de quem assumiu a role.

03

CAPÍTULO 3 · 34% DA PROVA

Domínio 3: Tecnologia e serviços da nuvem

Aqui eu preciso saber escolher o serviço certo para cada caso de uso: infraestrutura global, formas de acesso, EC2 e suas famílias, contêineres, serverless, bancos de dados, armazenamento e classes do S3, VPC e conectividade, integração de aplicações, monitoramento, IA/ML e analytics. É o maior domínio (34% da nota) e o enunciado sempre esconde um qualificador que decide (menor esforço operacional, sem gerenciar servidores, menor custo, controle do SO). Onde eu mais erro: Multi-AZ x réplica de leitura, SQS x SNS, NAT gateway x internet gateway, as classes do S3 e esquecer limites como os 15 minutos do Lambda e o EBS preso à AZ.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Infraestrutura global

Região é uma área geográfica com várias zonas de disponibilidade isoladas; cada AZ tem um ou mais data centers, a até 100 km entre si, ligados por fibra dedicada e redundante. Edge locations atendem CloudFront, Route 53 e Global Accelerator. Local Zones levam computação para perto de cidades, Wavelength para redes 5G e Outposts coloca racks gerenciados pela AWS no data center do cliente. IAM é global; EC2 é regional e cada instância e volume EBS fica numa única AZ.

Escolha de Região e uso de várias Regiões

Critérios: conformidade e residência de dados (lei decide primeiro), latência para os clientes, serviços disponíveis e preço. Várias Regiões servem para desastre regional, usuários em outro continente ou dado que deve ficar em outro país; falha de data center se resolve com várias AZs. A localização física dos dados é definida pela Região, não por AZ, VPC ou CloudFront.

Formas de acesso e infraestrutura como código

Console, CLI e SDKs chamam as mesmas APIs autenticadas: o IAM autoriza e o CloudTrail registra. Console serve a pessoas e tarefas pontuais; CLI e SDK, a scripts e pipelines. CloudFormation cria pilhas repetíveis com rollback; StackSets distribuem a mesma pilha em muitas contas e Regiões; o CDK escreve a infraestrutura em linguagem de programação e gera templates do CloudFormation.

Amazon EC2

AMI é o modelo com SO e software para iniciar instâncias; o tipo de instância define vCPU e memória. Famílias: C para CPU, R e X para memória, I, D e H para E/S em disco local, M e T para uso geral (T acumula créditos para picos), P e G com GPU. Graviton (Arm) dá melhor preço/desempenho sem compromisso. O IPv4 público automático muda a cada parada; IP fixo = Elastic IP.

Contêineres: ECS, EKS e Fargate

ECS é o orquestrador da própria AWS; com capacidade EC2 o cliente mantém controle do SO e da rede. EKS oferece o plano de controle do Kubernetes gerenciado e mantém kubectl, Helm e manifestos. Fargate é o modo serverless para ECS e EKS: a AWS cuida de provisionamento, patches e escala dos servidores; imagem, código, definição de tarefa e permissões continuam com o cliente.

Serverless e plataformas gerenciadas

Lambda executa funções por evento, cobra por requisições e duração em GB-segundo e tem limite de 15 minutos por invocação, que memória, concorrência provisionada ou imagem de contêiner não alteram. Jobs longos em fila vão para AWS Batch ou Fargate. API Gateway expõe APIs REST com chaves e throttling; Lambda@Edge roda código perto do usuário. Elastic Beanstalk implanta aplicação web tradicional com balanceamento e escala; Amplify hospeda front-end a partir do Git com CDN e back-end.

Auto Scaling e Elastic Load Balancing

Target tracking mantém uma métrica num valor (CPU em 50%); step scaling usa alarmes e degraus definidos pela equipe; ação agendada atende data e hora conhecidas; escalonamento preditivo aprende padrões recorrentes do histórico. ALB opera na camada 7 com regras por caminho, host ou cabeçalho; NLB na camada 4 (TCP/UDP, IP estático); Gateway Load Balancer insere appliances de terceiros no tráfego.

Amazon RDS e Aurora

RDS tira da equipe backups, patches de SO e mecanismo, instalação e failover; consultas, esquema, índices e regras de acesso continuam com o cliente. Multi-AZ é alta disponibilidade (a espera não atende leitura); réplica de leitura escala leitura. Aurora Serverless ajusta capacidade em ACUs para carga intermitente; Aurora Global Database dá leitura rápida em outro continente e recuperação de falha de Região.

Bancos de propósito específico

DynamoDB é NoSQL chave-valor serverless; modo sob demanda para tráfego imprevisível, provisionado para tráfego estável; DAX é cache em memória. Redshift é data warehouse colunar (OLAP). ElastiCache faz cache em memória para aliviar o banco. DocumentDB mantém drivers do MongoDB. Neptune percorre relacionamentos com muitos saltos (grafos). OpenSearch Service faz busca de texto em logs com painéis quase em tempo real.

Armazenamento em bloco e de arquivos

EBS é bloco persistente, serve de volume raiz, fica preso à AZ (mudar de AZ = snapshot e novo volume) e é cobrado pelo tamanho provisionado. Instance store é efêmero: mantém dados no reboot e perde no stop, hibernate ou terminate. EFS é NFS compartilhado para Linux. FSx for Windows File Server dá SMB com Active Directory; FSx for NetApp ONTAP atende NFS e SMB com SnapMirror. Storage Gateway integra o local ao S3: File (NFS/SMB), Volume (iSCSI) e Tape (fitas virtuais).

Amazon S3 e classes de armazenamento

S3 Standard guarda em no mínimo três AZs, com 11 noves de durabilidade e 99,99% de disponibilidade; não copia para outra Região sem S3 Replication. Standard-IA: acesso raro em milissegundos com taxa de recuperação; One Zone-IA: mais barato, uma AZ, para dados recriáveis; Intelligent-Tiering: padrão de acesso desconhecido, sem taxa de recuperação; Glacier Instant Retrieval: milissegundos, para arquivo consultado cerca de uma vez por trimestre; Glacier Flexible Retrieval: Expedited (minutos), Standard (horas) e Bulk (até 12 horas); Deep Archive: menor custo, restauração padrão em até 12 horas e em lote em até 48 horas, sem Expedited.

Recursos do S3

Versionamento recupera objeto sobrescrito ou apagado por engano. Object Lock impede exclusão por um prazo (WORM). Regras de ciclo de vida movem objetos para classes mais baratas por idade. Transfer Acceleration acelera uploads de longe pelo endpoint acelerado. Hospedagem de site estático atende sites sem lógica de servidor.

Componentes da VPC

Sub-rede pública é a associada a uma tabela de rotas com rota para um internet gateway; receber da internet exige IGW, rota e IP público ou Elastic IP. NAT gateway na sub-rede pública dá só saída IPv4 para sub-redes privadas; para IPv6, egress-only internet gateway. Gateway endpoint (só S3 e DynamoDB) não tem custo; interface endpoint (PrivateLink) é cobrado por hora e por GB. Aplicação pública segura = ALB público com instâncias em sub-redes privadas.

Conectividade entre redes

VPC peering liga poucas VPCs sem custo de conexão, não é transitivo e não aceita CIDR sobreposto. Transit Gateway é o hub para dezenas de VPCs, VPNs e Direct Connect. Site-to-Site VPN liga redes inteiras por IPsec na internet; Client VPN conecta funcionários remotos com cliente OpenVPN. Direct Connect é link dedicado sem internet pública; o Direct Connect gateway leva a várias VPCs. PrivateLink expõe um serviço específico a VPCs de outras contas.

Amazon Route 53 e entrega de conteúdo

Route 53 é DNS gerenciado, registra domínios e faz health checks. Políticas: simples (sem health check), ponderada (percentuais), latência (Região mais rápida), geolocalização (país ou continente, com registro padrão), failover e geoproximidade. CloudFront faz cache em edge locations; Global Accelerator otimiza o caminho até endpoints como ALB, NLB e EC2, sem cache.

Integração de aplicações e streaming

SQS é fila (pull) que guarda mensagens até o consumo; SNS é pub/sub (push) para fan-out, e-mail e SMS; EventBridge roteia eventos e agenda execuções (Scheduler); Step Functions orquestra fluxos com etapas, decisões e paralelismo. Kinesis Data Streams retém o stream para múltiplos consumidores independentes; Data Firehose entrega streaming ao S3 ou Redshift sem código. SES envia e-mail transacional com domínio próprio; Connect é central de atendimento na nuvem.

Monitoramento e operação

CloudWatch reúne métricas, logs, alarmes e dashboards; filtro de métricas conta padrões em logs. X-Ray mostra o caminho e o tempo de cada requisição entre microsserviços. Systems Manager gerencia instâncias sem SSH nem bastion (Session Manager, Run Command, Patch Manager). Health Dashboard informa eventos da AWS que afetam seus recursos; Service Quotas mostra limites e recebe pedidos de aumento; License Manager controla licenças por vCPU.

IA/ML e analytics

SageMaker AI prepara dados, treina e implanta modelos próprios; Bedrock dá acesso a modelos de base por API; Q Developer é assistente pronto para desenvolvedores. Serviços prontos: Transcribe (fala para texto), Polly (texto para fala), Translate, Comprehend (sentimento, entidades), Lex (bots com intenção), Textract (formulários e tabelas), Rekognition (imagem e vídeo). Analytics: Athena (SQL no S3 sem servidor), Glue (crawlers, catálogo e ETL), Redshift, Quick Sight (dashboards de BI) e EMR (Spark, Hadoop).

Macetes para memorizar

RDS

Multi-AZ Mantém no Ar (failover, a espera não lê); Read replica é para Relatório (escala leitura).

Mensageria

SQS é fila (pull, a mensagem espera o consumidor); SNS é megafone (push, avisa todos ao mesmo tempo); EventBridge é o relógio e o roteador de eventos; Step Functions é o maestro das etapas.

Famílias EC2

C = CPU, R = RAM, I = IOPS em disco local, T = Turbo nos picos com créditos, G e P = GPU, M = meio-termo.

Instance store x EBS

Instance store: reboot sobrevive, stop morre. EBS sobrevive ao stop, mas fica preso à AZ.

VPC

Sub-rede pública é questão de rota (rota para o IGW). NAT só deixa sair; para entrar, IGW + IP público ou ALB público. Gateway endpoint é grátis e só S3 e DynamoDB.

Route 53

Latência = o mais rápido; Geolocalização = de onde o usuário vem; Ponderado = percentual; Failover = reserva quando o primário cai.

Serviços de IA prontos

Transcribe escreve o que ouve; Polly fala o texto; Translate traduz; Comprehend compreende sentimento; Lex conversa; Textract extrai de formulários; Rekognition reconhece imagens. Treinar modelo próprio = SageMaker AI.

Classes do S3

Quanto mais frio, mais barato guardar e mais restrito recuperar: Standard (frequente), Standard-IA (raro, milissegundos, taxa por GB recuperado), Glacier Instant (cerca de uma vez por trimestre, milissegundos), Glacier Flexible (minutos a horas), Deep Archive (horas, sem Expedited). One Zone-IA = uma AZ, para dado recriável; padrão desconhecido = Intelligent-Tiering.

Tabela de memorização: não confunda

Quando é...	...e quando é
Amazon SQS Guardar trabalho até o consumidor processar no ritmo dele, sem perder mensagens se ele cair.	**Amazon SNS** Avisar pessoas ou vários assinantes ao mesmo tempo (fan-out, e-mail, SMS, alarme do CloudWatch).
RDS Multi-AZ Alta disponibilidade com failover automático; a instância em espera não atende leitura.	**Réplica de leitura do RDS** Tirar relatórios e consultas pesadas do banco principal, apontando para o endpoint da réplica.
AWS Fargate Contêineres sem gerenciar servidores, inclusive tarefas contínuas de horas.	**AWS Lambda** Funções curtas acionadas por eventos, até 15 minutos por invocação, pagando por requisição e duração.

Application Load Balancer Roteamento HTTP/HTTPS por caminho, host ou cabeçalho (camada 7).	**Network Load Balancer** TCP/UDP de alto desempenho, IP estático por AZ, latência ultrabaixa (camada 4).
VPC peering Duas ou poucas VPCs, comunicação direta e menor custo, sem ponto central.	**AWS Transit Gateway** Dezenas de VPCs e redes locais num hub central, eliminando a malha de peerings.
Amazon Athena Consultas SQL pontuais direto nos arquivos do S3, sem carregar dados nem gerenciar servidores.	**Amazon Redshift** Data warehouse com carga diária e BI intenso e contínuo de muitos analistas sobre terabytes.
Pilot light Só dados replicados e núcleo da infraestrutura ativos, servidores de aplicação desligados; recupera mais devagar.	**Warm standby** Cópia reduzida e totalmente funcional já rodando, escalada para assumir a produção.

Números que caem

Item	Valor
Peso do domínio na nota	**34%**
Tempo máximo de uma invocação do Lambda	**15 minutos (900 segundos), mesmo com 10.240 MB de memória**
Distância entre zonas de disponibilidade de uma Região	**Até 100 km, com fibra dedicada e redundante**
S3 Standard	**Mínimo de 3 AZs, 99,999999999% de durabilidade (11 noves) e 99,99% de disponibilidade**
S3 Glacier Flexible Retrieval	**Expedited em minutos; padrão de 3 a 5 horas**
S3 Glacier Deep Archive	**Restauração padrão em até 12 horas e em lote em até 48 horas, sem Expedited**
Frequência típica de acesso	**Standard-IA e One Zone-IA: acesso raro com recuperação em milissegundos; Glacier Instant Retrieval: cerca de uma vez por trimestre**
Atraso máximo de uma fila de atraso do SQS	**15 minutos**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Enviar relatórios para a instância em espera do RDS Multi-AZ.
Como não cair: A espera do Multi-AZ de instância serve só para failover. Escalar leitura = réplica de leitura.

⚠ **Alerta de prova:** Aumentar a memória, usar concorrência provisionada ou imagem de contêiner para rodar uma tarefa de horas no Lambda.
Como não cair: O limite de 900 segundos (15 minutos) vale em todos os casos. Tarefa longa = Fargate, EC2 ou Batch.

⚠ **Alerta de prova:** Usar NAT gateway para receber conexões da internet.
Como não cair: NAT gateway só permite saída de sub-redes privadas. Entrada exige internet gateway, rota e IP público, ou um ALB público na frente.

⚠ **Alerta de prova:** Desanexar o volume EBS e anexá-lo numa instância de outra AZ, ou usar Multi-Attach entre AZs.
Como não cair: EBS é preso à AZ, inclusive no Multi-Attach. Para outra AZ: snapshot e novo volume na AZ de destino.

⚠ **Alerta de prova:** Achar que o instance store mantém os dados quando a instância é parada.
Como não cair: Instance store perde dados no stop, hibernate ou terminate e só os mantém no reboot. Persistência após stop = EBS.

⚠ **Alerta de prova:** Acrescentar mais peerings achando que o tráfego passa de uma VPC para outra.
Como não cair: VPC peering não é transitivo e não aceita CIDR sobreposto. Hub central = Transit Gateway; serviço único para muitas VPCs = PrivateLink.

⚠ **Alerta de prova:** Escolher roteamento por geolocalização para mandar cada usuário à Região mais rápida.
Como não cair: Mais rápida = roteamento por latência com health checks. Geolocalização decide pelo país de origem (direitos de exibição, conteúdo por país).

⚠ **Alerta de prova:** Pensar que o S3 Standard grava numa única AZ ou replica para outra Região por padrão.
Como não cair: S3 Standard já usa no mínimo três AZs; uma AZ é a One Zone-IA. Outra Região só com S3 Replication configurada.

⚠ **Alerta de prova:** Usar Global Accelerator para acelerar uploads de equipes distantes para um bucket.
Como não cair: Upload lento para o S3 = S3 Transfer Acceleration. Global Accelerator atende endpoints como ALB, NLB e EC2.

⚠ **Alerta de prova:** Escolher endpoint de interface (PrivateLink) para o S3 quando o requisito é não ter custo de endpoint.
Como não cair: Gateway endpoint para S3 e DynamoDB é gratuito e entra na tabela de rotas; o de interface cobra por hora e por GB.

⚠ **Alerta de prova:** Configurar target tracking ou escalonamento preditivo para um pico único com data e hora conhecidas.
Como não cair: Target tracking reage depois que a carga sobe e o preditivo só aprende padrões recorrentes. Evento com hora marcada = ação agendada.

⚠ **Alerta de prova:** Usar Amazon Bedrock para treinar um modelo tabular próprio com algoritmos escolhidos pela equipe.
Como não cair: Bedrock dá modelos de base para IA generativa. Treinar e implantar modelo próprio com dados da empresa = SageMaker AI; tarefa comum por API pronta = serviço de IA específico.

⚠ **Alerta de prova:** Usar egress-only internet gateway para dar saída à internet a instâncias privadas que usam IPv4.
Como não cair: Egress-only internet gateway funciona só com IPv6. Saída IPv4 sem receber conexões = NAT gateway numa sub-rede pública.

⚠ **Alerta de prova:** Proteger backups de EBS, RDS e DynamoDB contra ransomware com S3 Object Lock ou com Backup Vault Lock no modo governança.
Como não cair: Pontos de recuperação ficam nos cofres do AWS Backup. Imutáveis até para o raiz = Backup Vault Lock no modo compliance; governança pode ser removida por quem tem permissão.

Como cai na prova

📝 **Como cai:** Cenário de aplicação com 'MAIS adequado' e 'menor esforço operacional' e alternativas que vão de EC2 a serverless.
Como resolver: Elimine primeiro o que exige gerenciar servidores (EC2, ECS em EC2). Entre os gerenciados, escolha pelo tipo de carga: função por evento até 15 minutos = Lambda; contêiner = Fargate; aplicação web tradicional = Elastic Beanstalk; front-end com Git e CDN = Amplify. Se pedir controle do SO ou de drivers, volte ao EC2.

📝 **Como cai:** Dados com padrão de acesso descrito e a pergunta 'qual classe do S3 ao menor custo?'.
Como resolver: Pergunte: com que frequência acessa? quanto tempo aceita esperar (milissegundos, minutos, horas)? o dado pode ser recriado (One Zone-IA)? o padrão é desconhecido (Intelligent-Tiering)? A classe mais barata que respeita o tempo de recuperação vence.

📝 **Como cai:** Instâncias em sub-rede privada precisando de algo (sair para a internet, receber usuários, falar com o S3).
Como resolver: Sair em IPv4 sem receber conexões = NAT gateway na sub-rede pública (IPv6 = egress-only IGW); receber usuários = ALB público com instâncias privadas; S3 ou DynamoDB sem internet e sem custo de endpoint = gateway endpoint.

📝 **Como cai:** Plano de recuperação de desastres com RTO e RPO informados e pedido de menor custo.
Como resolver: Horas de parada e de perda = backup e restauração; dezenas de minutos = pilot light; minutos com cópia reduzida rodando = warm standby; quase zero = multi-site ativo/ativo. Replicação contínua de servidores sem ambiente duplicado = Elastic Disaster Recovery.

📝 **Como cai:** Necessidade de IA descrita pela entrada e pela saída (áudio, texto, imagem, documento) e a pergunta 'qual serviço?'.
Como resolver: Identifique o formato de entrada e o que se quer na saída e escolha o serviço pronto correspondente. Só vá para SageMaker AI se o enunciado disser que nenhum serviço pronto resolve ou que a equipe quer treinar o próprio modelo; IA generativa por API = Bedrock; assistente de código = Q Developer.

📝 **Como cai:** Duas redes precisam se conectar e a pergunta 'qual serviço?'.
Como resolver: Veja quem conecta: notebook de funcionário = Client VPN; escritório ou data center pela internet = Site-to-Site VPN; link dedicado sem internet = Direct Connect; duas VPCs = peering; dezenas de VPCs e redes locais = Transit Gateway; um serviço exposto a muitas VPCs com CIDR sobreposto = PrivateLink.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Contêineres sem provisionar, atualizar ou escalar servidores	**AWS Fargate**
Manter kubectl, Helm e APIs do Kubernetes sem operar o plano de controle	**Amazon EKS**
Agendar uma execução diária ou reagir à mudança de estado de uma instância EC2	**Amazon EventBridge (Scheduler e regras)**
Fluxo com várias etapas, decisões, paralelismo e estado	**AWS Step Functions**
Streaming com retenção e vários consumidores independentes	**Amazon Kinesis Data Streams (sem código até o S3: Data Firehose)**
SQL interativo direto em arquivos do S3, sem servidores	**Amazon Athena**

Conteúdo estático com cache perto de usuários no mundo todo	**Amazon CloudFront**
Serviços da AWS rodando no data center do cliente por latência ou residência de dados	**AWS Outposts**
Servidores locais acessando por NFS ou SMB arquivos guardados no S3	**AWS Storage Gateway (File Gateway)**
Gerenciar instâncias sem SSH, sem bastion e sem IP público	**AWS Systems Manager**
Replicação contínua de servidores para DR com RPO de segundos e RTO de minutos	**AWS Elastic Disaster Recovery**
Desktop virtual persistente por usuário, sem comprar equipamentos	**Amazon WorkSpaces Personal (só uma aplicação pelo navegador: WorkSpaces Applications)**
Requisições com caminho /api para um grupo de destinos e /imagens para outro	**Application Load Balancer (camada 7)**
Cache em memória de dados muito lidos para aliviar o banco relacional	**Amazon ElastiCache**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Multi-AZ é failover e a espera não lê; escalar leitura é réplica de leitura.
- Lambda para em 15 minutos; tarefa de horas vai para Fargate, EC2 ou Batch.
- EBS fica preso à AZ e o instance store perde os dados no stop.
- NAT gateway só dá saída; entrada pela internet exige internet gateway, rota e IP público (ou ALB público).
- IAM é global, EC2 é regional e cada instância vive numa única AZ; a Região define onde os dados ficam.

Essenciais para a prova (checklist)

- ☐ Sei explicar Região, AZ, edge location, Local Zone e Outposts e qual escopo têm IAM, EC2 e EBS.
- ☐ Sei escolher a família de instância EC2 pelo gargalo (CPU, memória, disco local, picos, GPU).
- ☐ Sei quando usar EC2, ECS, EKS, Fargate, Lambda, Batch, Elastic Beanstalk e Amplify.
- ☐ Sei diferenciar Multi-AZ de réplica de leitura e escolher entre RDS, Aurora, DynamoDB, Redshift, ElastiCache, DocumentDB e Neptune.
- ☐ Sei escolher a classe do S3 pela frequência de acesso, tempo de recuperação e resiliência exigida.
- ☐ Sei separar EBS, instance store, EFS, FSx e Storage Gateway.
- ☐ Sei montar uma VPC com sub-rede pública, privada, NAT gateway, endpoints e security groups.

- ☐ Sei escolher entre peering, Transit Gateway, Site-to-Site VPN, Client VPN, Direct Connect e PrivateLink.
- ☐ Sei associar SQS, SNS, EventBridge, Step Functions, Kinesis e Firehose ao padrão de integração correto.
- ☐ Sei associar cada serviço de IA pronto à sua tarefa e quando usar SageMaker AI ou Bedrock.

Questões de revisão do capítulo

R3.1 · Domínio 3: Tecnologia e serviços da nuvem

No contexto do Amazon S3, qual recurso é mais adequado para reduzir custos ao armazenar grandes volumes de dados de backup que são acessados raramente, mas precisam ser recuperados de forma relativamente rápida quando necessário?

A. Utilizar a classe de armazenamento S3 Standard-IA (Infrequent Access)
B. Manter os dados na classe de armazenamento S3 Standard
C. Migrar os dados para o S3 Glacier Deep Archive
D. Habilitar o versionamento nos buckets S3

R3.2 · Domínio 3: Tecnologia e serviços da nuvem

Uma plataforma de streaming roda a mesma aplicação em São Paulo e em Frankfurt. Ela quer que cada usuário seja enviado à Região que responde mais rápido para ele e que, se a aplicação de uma Região ficar indisponível, o tráfego vá automaticamente para a outra. Qual configuração do Amazon Route 53 atende a esse requisito?

A. Roteamento ponderado (weighted), dividindo 50% das consultas para cada Região
B. Roteamento simples, com os endereços das duas Regiões no mesmo registro DNS
C. Roteamento baseado em latência, com health checks associados aos registros de cada Região
D. Roteamento por geolocalização, enviando cada continente a uma Região fixa definida pela equipe

R3.3 · Domínio 3: Tecnologia e serviços da nuvem

Uma empresa precisa distribuir conteúdo estático (como imagens e arquivos de estilo) globalmente com baixa latência para usuários em diferentes países. Ela também deseja que o conteúdo seja armazenado em cache próximo aos usuários para reduzir a carga nos servidores de origem. Qual serviço da AWS é MAIS adequado para essa necessidade?

A. Amazon CloudFront
B. Amazon S3
C. Elastic Load Balancing
D. AWS Global Accelerator

R3.4 · Domínio 3: Tecnologia e serviços da nuvem

Uma startup de logística quer projetar uma solução de ingestão de dados de sensores IoT em grande escala na AWS. Os dispositivos enviarão pequenos pacotes de telemetria continuamente, e a empresa precisa de: (1) alta disponibilidade global, (2) capacidade de escalar de forma elástica, (3) autenticação e autorização seguras por dispositivo, e (4) integração simplificada com outros serviços AWS para processamento em tempo quase real. Qual combinação de serviços é mais adequada para atender a esses requisitos, mantendo o menor esforço operacional possível para a equipe?

A. AWS IoT Core para conectar e autenticar os dispositivos e encaminhar os dados via regras
B. Kinesis Data Streams para ingestão e instâncias EC2 escaladas à mão para processar os registros
C. Um ALB em várias zonas recebendo conexões HTTP de cada dispositivo e gravando no banco
D. Amazon SNS recebendo as mensagens dos dispositivos e repassando a assinantes

Respostas comentadas

R3.1. A) Utilizar a classe de armazenamento S3 Standard-IA (Infrequent Access)

Por quê: A classe de armazenamento S3 Standard-IA (Infrequent Access) foi projetada exatamente para dados acessados com pouca frequência, mas que precisam estar disponíveis com baixa latência quando forem solicitados. Ela oferece custo de armazenamento menor que o S3 Standard, com pequena taxa por recuperação, sendo ideal para backups e dados usados esporadicamente.

✗ B) Incorreta. S3 Standard é otimizado para acesso frequente. Funciona, mas não é a opção mais econômica para dados raramente acessados, aumentando o custo total de armazenamento.

✗ C) Incorreta. S3 Glacier Deep Archive tem custo de armazenamento muito baixo, mas o tempo de recuperação é maior e o processo é voltado a arquivamento de longo prazo, não sendo ideal quando é necessária recuperação relativamente rápida.

✗ D) Incorreta. Habilitar versionamento aumenta a resiliência contra exclusão acidental, mas não reduz custos; na prática, pode até aumentá-los por manter múltiplas versões de objetos.

> **Dica de prova:** Standard: acesso frequente. Standard-IA e One Zone-IA: acesso raro com recuperação em milissegundos. Glacier Instant Retrieval: arquivo consultado cerca de uma vez por trimestre. Glacier Flexible Retrieval e Deep Archive: arquivamento com recuperação em minutos ou horas.

R3.2. C) Roteamento baseado em latência, com health checks associados aos registros de cada Região

Por quê: Com recursos em várias Regiões, o roteamento baseado em latência do Route 53 responde a cada consulta com a Região que oferece menor latência ao usuário. Ao associar health checks aos registros, o Route 53 só responde com endpoints saudáveis, o que dá failover automático entre as Regiões.

✗ A) Incorreta. O roteamento ponderado distribui as consultas por pesos definidos, útil para testes ou migrações graduais, e ignora qual Região é mais rápida para cada usuário.

✗ B) Incorreta. O roteamento simples devolve os valores do registro sem considerar latência e não suporta health checks, então não desvia o tráfego de uma Região com problema.

✗ D) Incorreta. A geolocalização decide pela localização de origem da consulta, não pela latência medida; um usuário pode ser enviado a uma Região que não é a mais rápida para ele.

> **Dica de prova:** Mais rápido para o usuário = latência. Onde o usuário está (país, continente) = geolocalização. Percentual de tráfego = ponderado.

R3.3. A) Amazon CloudFront

Por quê: O CloudFront é o serviço de Content Delivery Network (CDN) da AWS, projetado especificamente para entregar conteúdo (estático e dinâmico) com baixa latência e alta velocidade de transferência, utilizando uma rede global de edge locations. Ele também realiza cache do conteúdo próximo aos usuários, reduzindo a carga na origem (por exemplo, um bucket S3 ou um servidor web em EC2).

✗ B) Incorreta. Serviço de armazenamento de objetos altamente durável e escalável, mas não é, por si só, uma CDN global com cache em borda. Pode ser usado como origem do CloudFront, mas não substitui a função de CDN.

✗ C) Incorreta. Distribui tráfego entre instâncias (por exemplo, EC2) dentro de uma região ou VPC. Não faz distribuição global com cache em edge locations; seu foco é balanceamento de carga, não entrega de conteúdo em CDN.

✗ D) Incorreta. Melhora a disponibilidade e a performance de aplicações utilizando a rede global da AWS, porém não faz cache de conteúdo.

> **Dica de prova:** Quando a pergunta falar em "conteúdo estático", "baixa latência global" e "cache em edge locations", pense em Amazon CloudFront. Se falar em armazenar arquivos, lembre-se de Amazon S3; se falar em distribuir tráfego entre servidores, pense em Elastic Load Balancing.

R3.4. A) AWS IoT Core para conectar e autenticar os dispositivos e encaminhar os dados via regras

Por quê: O AWS IoT Core foi projetado para conectar dispositivos IoT em grande escala, com autenticação por certificado X.509, autorização baseada em políticas e alta disponibilidade gerenciada. Com o mecanismo de regras, os dados seguem para serviços como Amazon Data Firehose e Amazon S3, formando um pipeline gerenciado que escala automaticamente e exige pouco esforço operacional.

✗ B) Incorreta. Embora o Kinesis Data Streams seja adequado para ingestão em tempo real, delegar a autenticação e autorização de cada dispositivo para instâncias EC2 aumenta muito a complexidade e o esforço operacional.

✗ C) Incorreta. Application Load Balancer + EC2 para receber diretamente milhares ou milhões de conexões de dispositivos IoT exige grande esforço de gerenciamento de capacidade, patches, alta disponibilidade e segurança.

✗ D) Incorreta. O Amazon SNS é um serviço de mensagens pub/sub para distribuir notificações a assinantes; não oferece identidade por dispositivo com certificados, conexões MQTT persistentes nem o registro e o gerenciamento de dispositivos do...

Dica de prova: Quando o cenário envolver dispositivos IoT em grande escala com requisitos de autenticação por dispositivo, políticas de autorização específicas e conexão persistente (MQTT/HTTPS), priorize AWS IoT Core. Para armazenar grandes volumes de dados brutos, pense em Amazon S3;

04

CAPÍTULO 4 · 12% DA PROVA

Domínio 4: Cobrança, preços e suporte

Aqui eu preciso dominar as opções de compra do EC2 (sob demanda, Spot, RIs, Savings Plans, reservas de capacidade, hosts dedicados), como cada serviço é cobrado (Lambda, S3, EBS, transferência de dados), as ferramentas de custo (Cost Explorer, Budgets, Pricing Calculator, CUR, Cost Anomaly Detection), o faturamento consolidado, os planos de suporte atuais e os recursos de parceiros. É o menor domínio (12% da nota), mas são pontos quase garantidos se eu souber o verbo de cada ferramenta. Onde eu mais erro: misturar Cost Explorer, Budgets e Pricing Calculator, achar que reserva de capacidade dá desconto, usar Compute Savings Plans para bancos e lembrar dos nomes antigos dos planos de suporte.

Neste capítulo
15 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Opções de compra do EC2

Sob demanda: sem compromisso e sem interrupção, ideal para uso curto e imprevisível. Spot: o mais barato, mas pode ser interrompido com aviso de dois minutos; serve para jobs que param e recomeçam. Reserved Instances e Savings Plans: desconto por compromisso de 1 ou 3 anos para uso estável. Dedicated Hosts e Dedicated Instances atendem licença e isolamento e custam mais.

Reserved Instances

Standard dá o maior desconto, mas fica presa à família e ao SO; Convertible pode ser trocada por outra família, SO ou locação. A RI regional Linux com locação padrão vale em qualquer AZ da Região e tem flexibilidade de tamanho dentro da família (uma m5.2xlarge cobre duas m5.xlarge). A RI zonal reserva capacidade na AZ. All Upfront dá mais desconto; sem pagamento antecipado, a opção é No Upfront.

Savings Plans

Compromisso de gasto em US$/hora por 1 ou 3 anos, em quatro tipos. Compute Savings Plans: qualquer família, tamanho e Região, cobrindo EC2, Fargate e Lambda. EC2 Instance Savings Plans: presos a uma família numa Região. SageMaker AI Savings Plans: uso do SageMaker AI. Database Savings Plans: vários serviços de banco, com liberdade para trocar família, mecanismo e Região. Dão desconto, mas não reservam capacidade, e não reduzem o preço por GB do armazenamento do S3.

On-Demand Capacity Reservations

Garantem capacidade de um tipo de instância numa AZ escolhida, sem compromisso de prazo e com cancelamento livre. São cobradas pelo preço sob demanda, ou seja, não geram desconto sozinhas.

Como os serviços são cobrados

Lambda: número de requisições e duração em GB-segundo; sem invocação, sem custo de execução. S3: armazenamento por GB-mês, requisições, recuperação (classes IA e Glacier) e saída de dados; não há capacidade provisionada nem cobrança por bucket. EBS: tamanho provisionado, mesmo com a instância parada. O preço por GB cai em faixas mais altas de uso (preços em camadas).

Transferência de dados

Entrada de dados vinda da internet, em geral, não é cobrada. Saída para a internet é cobrada. Transferência entre Regiões é cobrada, mesmo dentro da rede da AWS (por exemplo, replicação entre Regiões).

Nível gratuito atual

Contas criadas desde 15/07/2025 escolhem entre os planos Free e Paid. No plano Free a conta não gera cobranças por até seis meses ou até acabarem os créditos, o que ocorrer primeiro, e não acessa alguns serviços nem compras de hardware. Clientes novos recebem US$ 100 em créditos e podem ganhar até mais US$ 100 concluindo atividades; '12 meses grátis' é o modelo antigo.

AWS Cost Explorer

Analisa custos e uso já ocorridos com gráficos e filtros por conta, tag e Região, e projeta gastos a partir do histórico. Traz recomendações de rightsizing para EC2, recomendações de compra de Savings Plans e RIs e relatórios de utilização e cobertura desses compromissos. Não envia alertas por limite nem desliga recursos.

AWS Budgets

Define orçamentos de custo ou uso e alerta por e-mail ou SNS quando o valor real ou previsto passa do limite. Tem orçamentos de utilização e de cobertura de RIs e Savings Plans. Budget actions, com aprovação manual ou automática, aplicam uma política do IAM, aplicam uma SCP (a partir da conta de gerenciamento) ou param instâncias EC2 ou RDS da conta.

Pricing Calculator, CUR e demais ferramentas

AWS Pricing Calculator estima o custo de algo que ainda não existe e compara cenários. Cost and Usage Report (CUR 2.0, via Data Exports) entrega dados detalhados de uso para S3, data warehouse e BI. Cost Anomaly Detection alerta gastos fora do padrão histórico. A página Bills mostra invoice em PDF, encargos por serviço e Região e status de pagamento. Compute Optimizer recomenda tamanhos para EC2, EBS e memória do Lambda com base no uso real.

Faturamento consolidado no AWS Organizations

A conta de gerenciamento paga as cobranças de todas as contas-membro numa fatura única e o uso agregado gera descontos por volume. Descontos de RIs e Savings Plans são compartilhados entre as contas por padrão; para excluir uma conta, a conta de gerenciamento desativa o compartilhamento nas preferências de faturamento.

Tags de alocação de custos e tag policies

Cost allocation tags detalham custos por projeto, ambiente ou centro de custo com mínimo esforço e sem custo adicional; Cost Explorer e Budgets usam essas tags. Tag policies do AWS Organizations padronizam chaves, capitalização e valores permitidos entre as contas.

Planos de suporte atuais

Basic (gratuito): atendimento 24x7 de conta e cobrança, verificações principais do Trusted Advisor, Health Dashboard, documentação e re:Post. Business Support+ (a partir de US$ 29 por mês): engenheiros 24x7 por telefone e chat, engajamento humano em menos de 30 minutos para sistema crítico fora do ar, Trusted Advisor completo, assistência com IA e Support API. Enterprise Support: TAM designado, resposta em até 15 minutos para casos críticos de produção e revisões estratégicas. Unified Operations: missão crítica, Domain Specialist Engineers, monitoramento proativo 24x7 e resposta em 5 minutos.

Recursos técnicos e de monitoramento da conta

Trusted Advisor verifica custo (recursos ociosos), desempenho, segurança, tolerância a falhas e limites de serviço. AWS Health Dashboard informa eventos e manutenções que afetam seus recursos; a AWS Health API os entrega por programa e exige Business Support+, Enterprise Support ou Unified Operations. AWS Support API abre e acompanha casos pelo código. re:Post e Knowledge Center respondem dúvidas técnicas no plano Basic. Abuso vindo de IPs da AWS se reporta ao AWS Trust & Safety.

Parceiros, Marketplace e Professional Services

Na AWS Partner Network, quem desenvolve e vende software é ISV; quem faz consultoria, migração e operação é parceiro de serviços (integrador). Ser parceiro dá treinamento e certificação, eventos e descontos por volume. AWS Marketplace vende software de terceiros com cobrança na fatura da AWS; private offer aplica preço e EULA negociados e Private Marketplace limita os times a produtos aprovados. AWS Professional Services é a equipe de especialistas da própria AWS contratada para o projeto.

Macetes para memorizar

Ferramentas de custo

Explorer explora o passado (e prevê pelo histórico); Budgets bota limite, avisa e pode agir; Calculator calcula o que ainda não existe; CUR é o dado bruto para BI.

Opções de compra

Spot = super barato, mas pode sumir com 2 minutos de aviso; sob demanda = sem compromisso e sem interrupção; RI e Savings Plans = casar por 1 ou 3 anos em troca de desconto.

Reserva de capacidade

On-Demand Capacity Reservation = lugar garantido na AZ, preço cheio. Savings Plans = desconto, sem lugar garantido.

Savings Plans

Compute SP é o coringa (EC2, Fargate e Lambda, qualquer família e Região); EC2 Instance SP fica preso a uma família na Região; banco de dados tem o próprio Database SP.

Reserved Instances

Convertible converte família, SO ou locação; Standard regional só ajusta o tamanho dentro da família. All Upfront = maior desconto; No Upfront = sem pagar antes.

Transferência de dados

Entrar é de graça; sair para a internet ou atravessar Regiões é pago.

Planos de suporte

Basic = básico grátis; Business Support+ = engenheiro 24x7 e menos de 30 minutos para sistema crítico fora do ar; Enterprise = TAM e 15 minutos; Unified Operations = 5 minutos e especialistas de domínio.

Armazenamento

EBS paga o que reservou (provisionado); S3 paga o que guardou (GB-mês, requisições e saída).

Tabela de memorização: não confunda

Quando é...	...e quando é
AWS Cost Explorer Quanto já gastei, tendências, previsão a partir do histórico e recomendações baseadas no uso da conta.	**AWS Pricing Calculator** Quanto vai custar um sistema que ainda não existe ou comparar cenários antes de criar recursos.
AWS Budgets Definir limite e ser avisado (ou agir) quando o gasto real ou previsto passar dele, inclusive utilização de Savings Plans abaixo da meta.	**AWS Cost Explorer** Analisar e visualizar custos, consultar relatórios de utilização e cobertura sem alerta automático.
Compute Savings Plans A carga vai mudar de família, tamanho ou Região, ou usar Fargate e Lambda.	**EC2 Instance Savings Plans / RI Standard** A família e a Região ficam estáveis e o objetivo é o maior desconto.
Reserved Instance Standard Configuração estável, buscando o maior desconto; na regional, troca só de tamanho dentro da família.	**Reserved Instance Convertible** Precisará mudar de família, sistema operacional ou locação durante o prazo.
Instâncias Spot Jobs em lote tolerantes a interrupção, ao menor custo possível.	**Instâncias sob demanda** Uso curto ou imprevisível que não aceita interrupção e não quer compromisso.
AWS Enterprise Support TAM designado, revisões estratégicas e resposta em até 15 minutos para casos críticos de produção.	**AWS Unified Operations** Missão crítica com Domain Specialist Engineers, monitoramento proativo 24x7 e resposta em 5 minutos.
AWS Professional Services Especialistas da AWS executando o projeto de migração junto com a equipe e transferindo conhecimento.	**Plano de suporte (TAM do Enterprise)** Orientação contínua e consultiva sobre a conta e resposta rápida a incidentes, sem executar o projeto.

Números que caem

Item	Valor
Peso do domínio na nota	**12%**
Prazo de Reserved Instances e Savings Plans	**1 ou 3 anos (não existe RI de 5 anos)**
Aviso de interrupção de instância Spot	**2 minutos**
Business Support+	**A partir de US$ 29 por mês; engajamento humano em menos de 30 minutos para sistema crítico fora do ar**
Enterprise Support	**Resposta em até 15 minutos para casos críticos de produção**

Unified Operations	**Resposta em 5 minutos (Incident Detection and Response), com TAM e Domain Specialist Engineers**
Planos Developer, Business e Enterprise On-Ramp	**Sem novas assinaturas e descontinuados em 01/01/2027**
Nível gratuito atual	**Contas desde 15/07/2025; plano Free sem cobrança por até 6 meses ou até acabarem os créditos; US$ 100 de créditos + até US$ 100 por atividades**
Flexibilidade de tamanho da RI regional Linux	**Uma m5.2xlarge cobre duas m5.xlarge na mesma família**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Escolher On-Demand Capacity Reservations para reduzir custo.
Como não cair: Reserva de capacidade garante capacidade e é cobrada a preço sob demanda. Desconto vem de Savings Plans ou RIs.

⚠ **Alerta de prova:** Usar Compute Savings Plans para cobrir RDS, Aurora ou DynamoDB.
Como não cair: Compute SP cobre EC2, Fargate e Lambda. Vários bancos com troca de mecanismo e Região = Database Savings Plans.

⚠ **Alerta de prova:** Achar que a RI regional perde o desconto ao trocar uma m5.2xlarge por duas m5.xlarge em AZs diferentes.
Como não cair: RI regional Linux com locação padrão tem flexibilidade de tamanho na família e vale em qualquer AZ. Trocar de família exige Convertible ou Savings Plan.

⚠ **Alerta de prova:** Usar a previsão do Cost Explorer para estimar um sistema que nunca rodou na conta.
Como não cair: A previsão projeta o histórico dos recursos existentes. Sistema novo = Pricing Calculator.

⚠ **Alerta de prova:** Esperar que Cost Explorer, Compute Optimizer ou Cost Anomaly Detection desliguem recursos.
Como não cair: Eles analisam, recomendam ou alertam. Agir no limite do orçamento = Budgets actions; ligar e desligar por horário = Instance Scheduler.

⚠ **Alerta de prova:** Aplicar SCP ou tag de custo para impedir que uma conta receba desconto de Savings Plans de outra.
Como não cair: O compartilhamento de descontos de RI e SP é desativado pela conta de gerenciamento nas preferências de faturamento.

⚠ **Alerta de prova:** Achar que uploads da internet são cobrados e que replicação entre Regiões é grátis por ficar na rede da AWS.
Como não cair: Entrada da internet em geral é grátis; saída para a internet e transferência entre Regiões são cobradas.

⚠ **Alerta de prova:** Supor que um volume EBS de 1.000 GB com 100 GB gravados é cobrado pelos 100 GB, ou que o S3 cobra uma capacidade reservada por bucket.
Como não cair: EBS cobra o tamanho provisionado (os 1.000 GB) até o volume ser excluído, inclusive volume solto de instância encerrada; o S3 não tem provisionamento e cobra os GB efetivamente guardados.

⚠ **Alerta de prova:** Achar que o plano Basic inclui casos técnicos com engenheiros ou TAM.
Como não cair: Basic cobre conta e cobrança, Trusted Advisor principal, Health Dashboard e re:Post. Engenheiros 24x7 começam no Business Support+; TAM só no Enterprise Support e no Unified Operations.

⚠ **Alerta de prova:** Responder '12 meses grátis com 750 horas de EC2' sobre o nível gratuito.
Como não cair: Esse é o modelo antigo. Hoje: planos Free e Paid, créditos de US$ 100 e plano Free sem cobrança por até seis meses ou até acabarem os créditos.

⚠ **Alerta de prova:** Escolher All Upfront quando o enunciado pede maior desconto sem pagamento antecipado obrigatório.
Como não cair: All Upfront exige pagar tudo no início. Maior desconto sem antecipação = 3 anos com No Upfront.

⚠ **Alerta de prova:** Usar o Trusted Advisor para pedir aumento de limite de serviço.
Como não cair: O Trusted Advisor só avisa que o limite está perto. Ver o valor aplicado e pedir aumento = Service Quotas.

⚠ **Alerta de prova:** Usar a verificação de otimização de instâncias reservadas do Trusted Advisor para ver como os descontos já contratados estão sendo aplicados entre as contas.
Como não cair: Essa verificação recomenda novas compras. Utilização e cobertura de RIs e Savings Plans entre contas = relatórios do Cost Explorer na conta de gerenciamento.

⚠ **Alerta de prova:** Comprar Savings Plans ou Instâncias Spot para garantir 40 instâncias numa AZ, sem compromisso de prazo.
Como não cair: Savings Plans exigem compromisso e não reservam capacidade; Spot pode faltar ou ser interrompida. Capacidade garantida sem prazo = On-Demand Capacity Reservation.

Como cai na prova

📝 **Como cai:** Requisito financeiro ('analisar gastos por tag', 'alerta quando passar do valor', 'estimar sistema novo', 'exportar para BI') e quatro ferramentas de custo.
Como resolver: Ache o verbo: analisar ou prever pelo histórico = Cost Explorer; alertar ou agir no limite = Budgets; estimar antes de existir = Pricing Calculator; dado detalhado para data warehouse = CUR 2.0; gasto fora do padrão = Cost Anomaly Detection; invoice e pagamento = página Bills.

📝 **Como cai:** Perfil de carga (estável, curta, interrompível, muda de família ou Região, precisa de capacidade numa AZ) e a pergunta 'qual opção de compra?'.
Como resolver: Aceita interrupção = Spot. Curta e sem compromisso = sob demanda. Estável por anos = RI ou Savings Plans; se muda família, Região ou usa Fargate e Lambda = Compute SP; se muda SO ou família numa RI = Convertible. Capacidade garantida sem prazo = Capacity Reservation (sem desconto).

📝 **Como cai:** Necessidades de suporte (TAM, tempo de resposta, engenheiro técnico) e a pergunta 'qual plano com o menor custo?'.
Como resolver: Liste a exigência mais alta: só conta, cobrança e documentação = Basic; engenheiro técnico 24x7 = Business Support+; TAM designado e 15 minutos = Enterprise Support; 5 minutos, monitoramento proativo e Domain Specialist Engineers = Unified Operations. Escolha o plano mais barato que cobre essa exigência.

📝 **Como cai:** Várias contas no AWS Organizations e dúvidas sobre quem paga e como os descontos são aplicados.
Como resolver: A conta de gerenciamento paga a fatura consolidada; o uso agregado gera desconto por volume; descontos de RI e SP são compartilhados por padrão e só a conta de gerenciamento desativa o compartilhamento. Utilização e cobertura = Cost Explorer; alerta de utilização baixa = Budgets.

📝 **Como cai:** Pergunta sobre quais componentes formam a fatura de um serviço (Lambda, S3, EBS) ou quais fluxos de dados são cobrados.
Como resolver: Lambda = requisições + duração em GB-segundo; S3 = GB-mês, requisições, recuperação e saída; EBS = tamanho provisionado, mesmo parado. Entrada da internet não é cobrada; saída para a internet e entre Regiões, sim.

📝 **Como cai:** Empresa busca ajuda externa (dúvida técnica, abuso, consultoria, software de terceiros, virar parceira) e a pergunta 'qual recurso?'.
Como resolver: Dúvida técnica sem plano pago = re:Post; abuso vindo de IPs da AWS = Trust & Safety; especialistas da AWS executando o projeto = Professional Services; software de terceiros na fatura = Marketplace; benefícios de parceiro = AWS Partner Network (ISV vende software, parceiro de serviços faz consultoria).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Jobs que podem ser interrompidos e reiniciados, ao menor custo	**Instâncias Spot**
Uso estável há mais de 12 meses, reduzir custo sem mudar a arquitetura	**Savings Plans ou Reserved Instances de 1 ou 3 anos**
Alertas por e-mail quando o gasto previsto passar de um valor, sem cortar serviço	**AWS Budgets**
Simular, planejar ou comparar cenários antes de criar recursos	**AWS Pricing Calculator**
Relatório detalhado de uso exportado para data warehouse e BI	**Cost and Usage Report (CUR 2.0 via Data Exports)**
Custos por projeto, ambiente ou centro de custo com mínimo esforço	**Tags de alocação de custos**
Várias contas, fatura única e desconto por volume agregado	**Faturamento consolidado do AWS Organizations**
Recursos ociosos: EC2 subutilizada, Elastic IP solto, load balancer sem uso	**AWS Trusted Advisor (otimização de custos)**
IPs da AWS fazendo varredura de portas contra seus servidores	**AWS Trust & Safety**
Dúvida técnica respondida pela comunidade, sem plano pago	**AWS re:Post**
Invoice em PDF do mês passado e status de pagamento	**Página Bills do Billing and Cost Management**
Preço negociado com fornecedor e catálogo só de produtos aprovados	**Private offer e Private Marketplace do AWS Marketplace**
E-mail quando menos de 90% do compromisso do Savings Plan for usado	**Orçamento de utilização de Savings Plans no AWS Budgets**
Quanto comprometer por hora em Savings Plans com base no uso recente da conta	**Recomendações de Savings Plans do AWS Cost Explorer**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Cost Explorer analisa o passado, Budgets alerta e age, Pricing Calculator estima o que ainda não existe.
- Capacity Reservation garante capacidade a preço sob demanda; desconto só com RI ou Savings Plans.
- Compute Savings Plans cobre EC2, Fargate e Lambda; bancos usam Database Savings Plans.
- Planos atuais: Basic, Business Support+, Enterprise Support (TAM) e Unified Operations; TAM não existe no Basic nem no Business Support+.
- Entrada de dados é grátis; saída para a internet e entre Regiões é paga.

Essenciais para a prova (checklist)

☐ Sei escolher entre sob demanda, Spot, RI, Savings Plans, Capacity Reservations e Dedicated Hosts para cada perfil de carga.

☐ Sei diferenciar RI Standard e Convertible, regional e zonal, e as opções de pagamento antecipado.

☐ Sei quais serviços cada tipo de Savings Plans cobre.

☐ Sei como Lambda, S3, EBS e transferência de dados são cobrados.

☐ Sei separar Cost Explorer, Budgets, Pricing Calculator, CUR, Cost Anomaly Detection e a página Bills.

☐ Sei quem paga a fatura consolidada e como funciona o compartilhamento de descontos na organização.

☐ Sei o que incluem Basic, Business Support+, Enterprise Support e Unified Operations.

☐ Sei diferenciar Trusted Advisor, Health Dashboard, Health API, Support API e re:Post.

☐ Sei diferenciar ISV, parceiro de serviços, AWS Marketplace e AWS Professional Services.

Questões de revisão do capítulo

R4.1 · Domínio 4: Cobrança, preços e suporte

Uma rede de hospitais vai migrar 300 aplicações e quer contratar especialistas da própria AWS para trabalhar junto com a equipe interna e com parceiros, desenhando a arquitetura, executando a migração e transferindo conhecimento ao time. Qual oferta atende?

A. AWS Activate, com créditos e orientação técnica para startups
B. AWS re:Post, com respostas de especialistas e da comunidade
C. AWS Professional Services, com especialistas da AWS no projeto
D. AWS Enterprise Support, com um gerente técnico de conta (TAM) designado

R4.2 · Domínio 4: Cobrança, preços e suporte

Uma empresa com várias contas no AWS Organizations compra software de terceiros pelo AWS Marketplace. A área de compras negociou com um fornecedor preço e contrato de licença (EULA) próprios e quer que os times possam assinar somente produtos aprovados. Quais recursos do AWS Marketplace atendem a essas necessidades?

A. Compra pelo preço público da listagem e AWS Service Catalog para publicar a lista de fornecedores aprovados
B. Oferta privada (private offer) com os termos negociados e Private Marketplace com produtos aprovados
C. Modelo BYOL na listagem do produto e tag policies do AWS Organizations para bloquear assinaturas não aprovadas
D. AWS Data Exchange para negociar o contrato e AWS Budgets para impedir assinaturas fora da lista aprovada

R4.3 · Domínio 4: Cobrança, preços e suporte

Uma empresa com o plano AWS Business Support+ quer um único lugar, já incluído no plano, que aponte recursos que geram custo sem uso: instâncias Amazon EC2 com baixa utilização, volumes Amazon EBS subutilizados, endereços Elastic IP não associados e load balancers ociosos. Qual serviço atende a essa necessidade?

A. AWS Health Dashboard, com eventos sobre os recursos da conta que estão sem uso
B. AWS Budgets, com alertas quando o gasto mensal previsto ultrapassar o valor orçado
C. AWS Trusted Advisor, com as verificações da categoria de otimização de custos
D. AWS Pricing Calculator, com estimativas comparando a configuração atual e a ideal

R4.4 · Domínio 4: Cobrança, preços e suporte

Uma empresa de comércio eletrônico está avaliando como controlar melhor seus gastos em AWS e definir limites de uso por centro de custo (como Marketing, TI e Analytics). Ela quer receber alertas quando o consumo projetado ultrapassar um determinado valor mensal, sem impedir automaticamente a continuidade dos serviços. Qual combinação de recursos da AWS é mais adequada para atender a esse requisito?

A. Criar um AWS Organizations com contas separadas por centro de custo e usar Service Control Policies (SCPs) para bloquear recursos quando o gasto projetado ultrapassar o limite
B. Ativar o AWS Trusted Advisor para receber alertas quando o gasto projetado passar do limite
C. Criar Cost Allocation Tags, configurar AWS Budgets com alertas por e-mail ou SNS e usar relatórios do AWS Cost Explorer por tag
D. Usar o AWS Cost Anomaly Detection por centro de custo, sem criar tags

Respostas comentadas

R4.1. C) AWS Professional Services, com especialistas da AWS no projeto

Por quê: O AWS Professional Services reúne consultores e especialistas da AWS que atuam em projetos do cliente, muitas vezes em conjunto com parceiros da AWS, para desenhar, migrar e modernizar cargas de trabalho. É diferente do suporte (Enterprise Support e TAM), que orienta e responde casos, e da comunidade re:Post.

✗ A) Incorreta. O AWS Activate é um programa de créditos e recursos para startups, não um serviço de consultoria para migrações de grandes empresas.

✗ B) Incorreta. O re:Post é um serviço de perguntas e respostas da comunidade; não há equipe dedicada trabalhando no projeto.

✗ D) Incorreta. O TAM do Enterprise Support orienta e acompanha a conta de forma consultiva, mas não executa um projeto de migração de 300 aplicações.

> **Dica de prova:** Quer a AWS executando o projeto com a sua equipe = Professional Services. Quer orientação contínua e resposta rápida = plano de suporte.

R4.2. B) Oferta privada (private offer) com os termos negociados e Private Marketplace com produtos aprovados

Por quê: O AWS Marketplace oferece recursos de governança e gestão de licenças para compradores: ofertas privadas com preço e EULA negociados, Private Marketplace para catálogos de produtos aprovados por conta ou unidade organizacional e integração com o AWS License Manager para distribuir licenças (entitlements) entre as contas. As cobranças aparecem na fatura da AWS.

✗ A) Incorreta. Comprar pelo preço público ignora a negociação feita; e o Service Catalog organiza produtos de TI aprovados para implantação, mas não aplica o preço negociado nem controla assinaturas no Marketplace.

✗ C) Incorreta. BYOL usa uma licença comprada fora do Marketplace, e tag policies padronizam tags; nenhum dos dois restringe quais produtos os times podem assinar.

✗ D) Incorreta. O AWS Data Exchange é para produtos de dados de terceiros, e o AWS Budgets acompanha gastos com alertas e ações; nenhum dos dois limita as assinaturas a um catálogo aprovado.

> **Dica de prova:** Preço negociado = oferta privada. Catálogo de produtos aprovados = Private Marketplace. Licenças compartilhadas entre contas = License Manager.

R4.3. C) AWS Trusted Advisor, com as verificações da categoria de otimização de custos

Por quê: O AWS Trusted Advisor inspeciona a conta e recomenda melhorias em otimização de custos, desempenho, segurança, tolerância a falhas, cotas de serviço e excelência operacional. O plano Basic tem só as verificações principais; Business Support+, Enterprise e Unified Operations têm o conjunto completo, que inclui as verificações de custo de recursos ociosos.

✗ A) Incorreta. O AWS Health Dashboard informa eventos de serviços da AWS e mudanças programadas que afetam a conta, não recursos ociosos que geram custo.

✗ B) Incorreta. O AWS Budgets avisa quando o custo real ou previsto ultrapassa um limite, mas não identifica quais recursos estão ociosos.

✗ D) Incorreta. A Pricing Calculator estima custos de arquiteturas planejadas; ela não analisa os recursos que já existem na conta.

> **Dica de prova:** Lista de recursos ociosos ou subutilizados para cortar custo = Trusted Advisor (otimização de custos). Alerta de gasto = Budgets.

R4.4. C) Criar Cost Allocation Tags, configurar AWS Budgets com alertas por e-mail ou SNS e usar relatórios do AWS Cost Explorer por tag

Por quê: Cost Allocation Tags (como CostCenter=Marketing) separam os custos por área; o AWS Budgets cria orçamentos filtrados por essas tags e envia alertas por e-mail ou Amazon SNS quando o gasto real ou previsto ultrapassa o limite, sem interromper os serviços; e o Cost Explorer mostra os custos agrupados por tag. É a combinação que dá controle por centro de custo com alertas.

✗ A) Incorreta. Separar contas ajuda na governança, mas a empresa quer alertas, não bloqueio; usar SCPs para barrar recursos contraria o requisito de não interromper os serviços.

✗ B) Incorreta. O Trusted Advisor recomenda otimizações de custo, como recursos ociosos, mas não acompanha orçamentos por centro de custo nem alerta sobre gasto projetado.

✗ D) Incorreta. O Cost Anomaly Detection usa aprendizado de máquina para avisar sobre gastos fora do padrão histórico; não alerta quando o consumo projetado ultrapassa um valor mensal definido, papel do AWS Budgets.

> **Dica de prova:** Para a prova CLF-C02, lembre-se: "Alertas de orçamento" = AWS Budgets; "Análise visual de custos" = Cost Explorer; "Rastrear custos por área/projeto" = Cost Allocation Tags.

DIA DA PROVA

Estratégia de prova

O CLF-C02 é um exame de fundamentos: codificação, design de arquitetura em nuvem, solução de problemas, implementação e testes de carga e de desempenho estão fora do escopo. Cada pergunta traz um cenário curto de negócio e pede o serviço, o recurso, o pilar ou a responsabilidade que atende ao requisito. Os distratores são da mesma área e muitas vezes funcionariam, mas falham num detalhe do enunciado, como esforço operacional, custo, escopo (AZ ou Região, conta ou organização) ou prazo de compromisso. A banca mede se você associa necessidade a serviço com precisão e se entende o que muda entre um serviço gerenciado e um autogerenciado. Segurança (30%) e Tecnologia (34%) somam quase dois terços da nota.

Como responder

✓ Controle o tempo: são 65 perguntas em 90 minutos, cerca de 1 minuto e 20 segundos por pergunta. Responda na primeira passada, marque as duvidosas e volte no fim.

✓ Leia primeiro a frase final para saber o que está sendo pedido e depois sublinhe o qualificador decisivo: MAIS adequado, menor custo, menor esforço operacional, sem gerenciar servidores, sem compromisso, sem interrupção.

✓ Elimine pela categoria: se o requisito é auditoria, descarte serviços de proteção de DDoS; se é estimar custo futuro, descarte ferramentas de análise histórica. Costumam sobrar duas opções vizinhas.

✓ Entre duas opções que funcionam, prefira a gerenciada ou serverless quando o enunciado fala em esforço operacional mínimo, e a autogerenciada (EC2) quando exige controle do SO, de drivers ou do banco.

✓ Nas perguntas de múltipla resposta, o enunciado indica quantas marcar (Escolha DUAS). Julgue cada alternativa como verdadeira ou falsa isoladamente antes de comparar.

✓ Nunca deixe em branco: não há penalidade por chute. As 15 perguntas não pontuadas não são identificadas, então uma pergunta estranha não deve abalar o ritmo.

✓ Desconfie de absolutos e de promessas impossíveis: '100% de disponibilidade garantida', 'desconto sem compromisso', 'a AWS assume toda a segurança'.

✓ Use os nomes atuais: AWS Security Hub CSPM, Amazon SageMaker AI, Amazon Quick Sight, WorkSpaces Applications (ex-AppStream 2.0) e os planos Basic, Business Support+, Enterprise Support e Unified Operations.

Erros que derrubam candidatos

✗ Trocar CloudTrail (quem fez a chamada), Config (como estava configurado) e CloudWatch (métricas, logs e alarmes).

✗ Supor que serviço gerenciado ou serverless transfere à AWS dados, identidades, security groups e criptografia.

✗ Misturar Cost Explorer (analisa), Budgets (alerta e age) e Pricing Calculator (estima antes).

✗ Escolher uma solução que funciona, mas não é a mais adequada ao qualificador, como EC2 com ALB configurado à mão quando o pedido é mínimo esforço operacional.

✗ Ignorar o escopo do enunciado: falha de AZ x desastre regional, uma conta x organização inteira, alerta x bloqueio.

✗ Responder com conhecimento desatualizado: '12 meses grátis', planos Developer e Enterprise On-Ramp, Snowball Edge e Migration Hub para clientes novos.

✗ Confundir princípios de design parecidos entre pilares do Well-Architected, como game day em Excelência Operacional, Confiabilidade e Segurança.

Na semana da prova

- ☐ Refaça os simulados e revise só os erros, anotando o par 'resposta certa x alternativa que me enganou' e o detalhe que separa as duas.
- ☐ Revise as tabelas de pares que mais derrubam: CloudTrail/Config/CloudWatch; GuardDuty/Inspector/Macie/Detective; SQS/SNS/EventBridge; Multi-AZ/réplica de leitura; classes do S3; Budgets/Cost Explorer/Pricing Calculator.
- ☐ Memorize as listas fechadas: seis vantagens da nuvem, seis pilares e seus princípios, seis perspectivas e quatro fases do CAF, os 7 Rs de migração e o que cada plano de suporte inclui.
- ☐ Na véspera, não estude assunto novo; confira agendamento e documentos e descanse.
- ☐ No dia, mantenha o ritmo de cerca de 1 minuto e 20 segundos por pergunta, marque as dúvidas e reserve os minutos finais para revisá-las sem deixar nada em branco.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Domínio 1: Conceitos da nuvem

‣ Comprava servidores para o pico e ficava com capacidade ociosa ou faltando → **Parar de adivinhar a capacidade**

‣ Uso agregado de centenas de milhares de clientes reduz o preço → **Economias de escala**

‣ Atender clientes de outro país em poucos dias, sem data center no exterior → **Tornar-se global em minutos (Região próxima)**

‣ Sem especialistas em ML, NoSQL ou mídia, a empresa consome a tecnologia como serviço em vez de formar equipe para hospedá-la → **Democratizar tecnologias avançadas (Eficiência de Performance)**

‣ Escolher o banco pela forma como os dados são lidos e gravados → **Afinidade mecânica (mechanical sympathy)**

⚠ No EC2 o SO convidado continua sendo do cliente. Saem apenas os custos físicos (energia, espaço, troca de discos e fontes); licenças e código continuam.

⚠ Economia de escala explica só o preço menor pelo uso agregado. Capacidade ociosa ou insuficiente é 'parar de adivinhar a capacidade'; chegar antes ao mercado é velocidade e agilidade (time to market).

⚠ RI é desconto de cobrança com prazo de 1 ou 3 anos. O hardware é sempre da AWS e o cliente troca de geração de instância quando quiser.

2. Domínio 2: Segurança e conformidade

‣ Quem excluiu o recurso e em que horário a chamada foi feita → **AWS CloudTrail**

‣ Histórico ou linha do tempo de configuração para conformidade → **AWS Config**

‣ Impedir mesmo administradores das contas-membro → **Service Control Policies no AWS Organizations**

‣ Relatórios SOC, ISO ou PCI da própria AWS para auditores → **AWS Artifact**

‣ CPF, cartões ou dados pessoais em buckets do S3 → **Amazon Macie**

⚠ SCP só limita, nunca concede. Acesso exige role ou permission set do IAM Identity Center.

⚠ Security group só tem regras de permissão. Negar IP específico na sub-rede = network ACL; por taxa de requisições HTTP = WAF rate-based.

⚠ Config detecta e alerta depois do fato. Impedir a ação, até para administradores, é SCP no AWS Organizations.

3. Domínio 3: Tecnologia e serviços da nuvem

‣ Contêineres sem provisionar, atualizar ou escalar servidores → **AWS Fargate**

‣ Manter kubectl, Helm e APIs do Kubernetes sem operar o plano de controle → **Amazon EKS**

‣ Agendar uma execução diária ou reagir à mudança de estado de uma instância EC2 → **Amazon EventBridge (Scheduler e regras)**

‣ Fluxo com várias etapas, decisões, paralelismo e estado → **AWS Step Functions**

‣ Streaming com retenção e vários consumidores independentes → **Amazon Kinesis Data Streams (sem código até o S3: Data Firehose)**

⚠ A espera do Multi-AZ de instância serve só para failover. Escalar leitura = réplica de leitura.

⚠ O limite de 900 segundos (15 minutos) vale em todos os casos. Tarefa longa = Fargate, EC2 ou Batch.

⚠ NAT gateway só permite saída de sub-redes privadas. Entrada exige internet gateway, rota e IP público, ou um ALB público na frente.

4. Domínio 4: Cobrança, preços e suporte

‣ Jobs que podem ser interrompidos e reiniciados, ao menor custo → **Instâncias Spot**

‣ Uso estável há mais de 12 meses, reduzir custo sem mudar a arquitetura → **Savings Plans ou Reserved Instances de 1 ou 3 anos**

‣ Alertas por e-mail quando o gasto previsto passar de um valor, sem cortar serviço → **AWS Budgets**

‣ Simular, planejar ou comparar cenários antes de criar recursos → **AWS Pricing Calculator**

‣ Relatório detalhado de uso exportado para data warehouse e BI → **Cost and Usage Report (CUR 2.0 via Data Exports)**

⚠ Reserva de capacidade garante capacidade e é cobrada a preço sob demanda. Desconto vem de Savings Plans ou RIs.

⚠ Compute SP cobre EC2, Fargate e Lambda. Vários bancos com troca de mecanismo e Região = Database Savings Plans.

⚠ RI regional Linux com locação padrão tem flexibilidade de tamanho na família e vale em qualquer AZ. Trocar de família exige Convertible ou Savings Plan.

GABARITO

Respostas do diagnóstico

D1. D) Menos horas da equipe em tarefas operacionais como patches e backups → revise o capítulo 1

Por quê: Serviços gerenciados reduzem o custo total de propriedade porque transferem para a AWS tarefas repetitivas que consomem horas da equipe: no Amazon RDS, a AWS gerencia backups, patches de software e do sistema operacional, detecção de falhas e recuperação. Uma comparação que olha só o preço por hora ignora esse custo de pessoas, que muitas vezes é o maior.

✗ A) Incorreta. A instância do RDS costuma ter preço por hora maior que uma instância EC2 de mesmo porte, justamente porque inclui a gestão do banco.

✗ B) Incorreta. O RDS for MySQL usa a edição Community do MySQL; não há licença Enterprise embutida no preço.

✗ C) Incorreta. O armazenamento do RDS é cobrado à parte, por GB provisionado por mês.

> **Dica de prova:** Ao comparar EC2 autogerenciado com serviço gerenciado, some as horas de administração: é ali que o gerenciado costuma ganhar.

D2. B) Quando a demanda de recursos de TI é altamente variável e imprevisível ao longo do tempo → revise o capítulo 1

Por quê: O modelo pay-as-you-go é ideal quando a demanda é variável ou imprevisível: a empresa paga pelo que consome e aumenta ou reduz a capacidade rapidamente, sem grandes investimentos iniciais em hardware. Elasticidade e pagamento sob demanda alinham os custos ao uso real, enquanto a infraestrutura própria exige dimensionar para o pico.

✗ A) Incorreta. Investimento inicial elevado e depreciação de servidores são típicos de ambiente on-premises com CAPEX alto. Isso vai contra a proposta do pay-as-you-go, que reduz o investimento inicial e converte gastos em custos operacionais...

✗ C) Incorreta. Se a capacidade não vai mudar por muitos anos, o benefício de elasticidade e pagamento sob demanda é pouco aproveitado; nesse caso, compromissos de longo prazo ou infraestrutura própria podem fazer sentido.

✗ D) Incorreta. Exigir a propriedade física dos servidores e storages caracteriza um ambiente on-premises ou colocation. No modelo pay-as-you-go, os recursos de nuvem são gerenciados e fisicamente mantidos pela AWS, não pelo cliente.

> **Dica de prova:** Associe pay-as-you-go a demanda variável ou imprevisível, picos sazonais, projetos piloto e a evitar investimento inicial (CAPEX).

D3. B) AWS DataSync, com agente no ambiente local e tarefas agendadas de transferência → revise o capítulo 1

Por quê: O AWS DataSync é o serviço de transferência online de arquivos e objetos para, de e entre serviços de armazenamento da AWS. Um agente instalado no ambiente local lê o armazenamento (NFS, SMB, HDFS, objetos), e o serviço automatiza a transferência com protocolo próprio e paralelismo, criptografia e validação de integridade. É indicado para migrar, replicar e arquivar grandes volumes pela rede.

✗ A) Incorreta. O Transfer Acceleration acelera uploads de clientes distantes para um bucket, mas não lê um servidor NFS, não agenda tarefas e não faz cópia incremental.

✗ C) Incorreta. O File Gateway dá acesso híbrido contínuo, por NFS ou SMB, a arquivos guardados no S3; ele não é a ferramenta de migração em massa com tarefas agendadas e verificação de integridade.

✗ D) Incorreta. O Snowball Edge transfere dados offline por dispositivo físico e, desde novembro de 2025, não aceita novos clientes; a empresa quer transferir pela rede.

> **Dica de prova:** Mover grandes volumes de arquivos do data center para S3, EFS ou FSx pela rede, com agendamento e verificação = DataSync. Acesso híbrido contínuo = Storage Gateway.

D4. B) Chave gerenciada pelo cliente no AWS KMS, com política de chave e rotação definidas pela empresa → revise o capítulo 2

Por quê: O AWS KMS tem três tipos de chave: gerenciadas pelo cliente (controle total da política, do ciclo de vida e da rotação, com cobrança mensal por chave), gerenciadas pela AWS (criadas por um serviço na sua conta, com alias aws/serviço, política controlada pelo serviço e rotação anual obrigatória) e de propriedade da AWS (em contas do serviço, sem visibilidade nem custo). Quando a exigência é controle, a escolha é a chave gerenciada pelo cliente.

✗ A) Incorreta. Chaves de propriedade da AWS ficam em contas da AWS; o cliente não vê nem gerencia a política, a rotação ou o uso delas.

✗ C) Incorreta. Chaves gerenciadas pela AWS têm a política controlada pelo serviço: o cliente pode vê-la e auditar o uso, mas não pode alterá-la, desabilitar a chave nem mudar a rotação anual.

✗ D) Incorreta. Guardar as chaves no próprio volume enfraquece a proteção e não oferece controle central por política nem trilha de auditoria como o KMS.

> **Dica de prova:** Precisa controlar a política, desabilitar ou rotacionar no seu ritmo = chave gerenciada pelo cliente. Alias aws/serviço = gerenciada pela AWS, sem esse controle.

D5. D) Usar trilha da organização com logs em conta central e SCP que impede alterar o CloudTrail → revise o capítulo 2

Por quê: Uma trilha da organização no AWS CloudTrail registra os eventos de todas as contas e envia os logs para um bucket S3 em uma conta central de logging, e as contas-membro não podem alterá-la. Uma Service Control Policy (SCP) aplicada na organização nega ações como StopLogging e DeleteTrail, e esse limite vale até para administradores das contas-membro.

✗ A) Incorreta. Políticas IAM baseadas em identidade podem ser sobrescritas ou ajustadas por administradores locais com privilégios elevados.

✗ B) Incorreta. Uma regra do AWS Config detecta e alerta depois que o CloudTrail é desativado, mas não impede a ação; até a correção, a conta fica sem auditoria.

✗ C) Incorreta. StackSets ajudam na padronização da configuração, mas não são um controle de segurança à prova de administradores da conta.

> **Dica de prova:** Para o exame Cloud Practitioner, memorize: quando a pergunta fala em impedir que até administradores da conta façam algo, a resposta quase sempre envolve AWS Organizations + Service Control Policies (SCP). IAM controla o que um principal PODE fazer;

D6. A) Anexar uma função (role) do IAM à instância → revise o capítulo 2

Por quê: Uma role do IAM anexada à instância, por meio de um perfil de instância, fornece credenciais temporárias rotacionadas automaticamente, sem chaves de longo prazo. Guardar chaves de um usuário IAM, no código ou no Secrets Manager, mantém credenciais permanentes que podem vazar, e liberar o bucket pelo IP público não identifica a aplicação e falha quando o IP muda.

✗ B) Incorreta. Chaves fixas no código podem vazar.

✗ C) Incorreta. Tira as chaves do código, mas elas continuam sendo credenciais de longo prazo que precisam de rotação e podem vazar.

✗ D) Incorreta. O IP público pode mudar e não identifica a aplicação; o acesso deve ser dado a uma identidade do IAM.

> **Dica de prova:** Permissão para aplicação em EC2: role do IAM, nunca chaves no código.

D7. D) Bloqueia a entrada e permite a saída → revise o capítulo 3

Por quê: Um grupo de segurança novo não tem regras de entrada, então bloqueia todo o tráfego de entrada, e tem uma regra de saída que permite todo o tráfego de saída. Como é stateful, as respostas ao tráfego de saída são liberadas automaticamente. Para aceitar conexões, é preciso adicionar regras de entrada explícitas.

✗ A) Incorreta. A entrada precisa de regras explícitas.

✗ B) Incorreta. É o inverso do comportamento padrão.

✗ C) Incorreta. A regra de saída padrão permite o tráfego de saída.

> **Dica de prova:** Grupo de segurança novo: entrada bloqueada, saída liberada.

D8. B) Amazon SQS → revise o capítulo 3

Por quê: O Amazon Simple Queue Service é um serviço totalmente gerenciado de filas de mensagens que permite comunicação assíncrona entre componentes desacoplados. Ele armazena mensagens de forma durável até que sejam processadas e excluídas, o que garante que nenhuma mensagem seja perdida quando consumidores estiverem temporariamente indisponíveis. É ideal para aumentar a resiliência e a escalabilidade de arquiteturas baseadas em microsserviços.

✗ A) Incorreta. Orquestra fluxos de trabalho e coordena serviços da AWS usando máquinas de estados. Embora possa chamar serviços em sequência e tratar erros, não é um serviço de fila de mensagens para desacoplamento genérico de produtores e...

✗ C) Incorreta. É um barramento de eventos para roteamento baseado em regras, ideal para arquiteturas orientadas a eventos. Ele não é projetado principalmente como fila de mensagens durável para garantir processamento assíncrono com controle...

✗ D) Incorreta. É um serviço de pub/sub para envio de notificações e mensagens em modo de difusão (fan-out) para múltiplos assinantes, mas não é uma fila de mensagens com armazenamento independente por consumidor.

> **Dica de prova:** Quando a questão falar em fila, mensagens assíncronas, desacoplamento e armazenamento confiável até o consumo, pense em Amazon SQS. Quando aparecer notificações para múltiplos destinos (fan-out), pense em Amazon SNS.

D9. D) Amazon Redshift, um data warehouse com armazenamento colunar e processamento paralelo → revise o capítulo 3

Por quê: Bancos OLTP, como o Amazon RDS, atendem muitas transações curtas (inserir uma venda, atualizar um pedido). Cargas OLAP fazem poucas consultas pesadas que agregam grandes volumes históricos, e para isso o Amazon Redshift usa armazenamento colunar e processamento paralelo em vários nós. Separar as análises num data warehouse evita disputar recursos com o sistema transacional.

✗ A) Incorreta. O DynamoDB é um banco NoSQL de chave-valor para acessos de baixa latência por chave, não para consultas analíticas com junções e agregações amplas.

✗ B) Incorreta. O ElastiCache acelera leituras repetidas com cache em memória, mas não executa consultas analíticas sobre o histórico completo.

✗ C) Incorreta. Uma réplica de leitura tira carga do banco principal, mas continua sendo um banco OLTP orientado a linhas, pouco eficiente para agregações sobre terabytes de histórico.

> **Dica de prova:** Transações do dia a dia = RDS/Aurora (OLTP). Relatórios e BI sobre terabytes de histórico = Redshift (OLAP, data warehouse).

D10. B) AWS Cost Explorer → revise o capítulo 4

Por quê: O AWS Cost Explorer permite visualizar e analisar custos e uso da AWS ao longo do tempo, com gráficos interativos e filtros por tag, conta vinculada, região, tipo de instância e outros atributos. É a ferramenta para entender onde o dinheiro está sendo gasto e apoiar a otimização de custos.

✗ A) Incorreta. Permite consolidar a cobrança de múltiplas contas em uma fatura única e aproveitar descontos agregados, mas não oferece, por si só, recursos avançados de análise gráfica e filtragem detalhada como o Cost Explorer.

✗ C) Incorreta. Focado em definir limites de gastos e gerar alertas quando o orçamento ou uso se aproxima ou excede esses limites. Não é a ferramenta principal para análise detalhada de custos históricos por serviço e tag.

✗ D) Incorreta. Serve para estimar custos futuros com base em configurações planejadas de serviços, não para analisar custos já incorridos ou detalhar despesas atuais por conta, tag ou região.

> **Dica de prova:** Para a prova, associe: Cost Explorer = análise detalhada de custos reais, Budgets = alertas e limites de gastos, Pricing Calculator = estimativas de custos futuros e Consolidated Billing = fatura única e descontos por volume.

D11. C) A conta de gerenciamento paga as cobranças geradas pelas contas-membro, numa fatura consolidada → revise o capítulo 4

Por quê: No AWS Organizations, toda organização tem uma conta de gerenciamento que paga as cobranças de todas as contas-membro. O faturamento consolidado entrega uma fatura única, permite acompanhar os custos por conta, agrega o uso para descontos por volume e compartilhamento de RI e Savings Plans, e não tem custo adicional.

✗ A) Incorreta. Administradores delegados recebem permissão para gerenciar serviços específicos da organização, não a responsabilidade de pagamento.

✗ B) Incorreta. Descontos de RI e Savings Plans podem ser compartilhados na organização, mas quem paga a fatura consolidada é a conta de gerenciamento.

✗ D) Incorreta. Com faturamento consolidado as contas-membro não pagam faturas próprias; a cobrança é concentrada na conta de gerenciamento.

> **Dica de prova:** Quem paga a conta da organização = conta de gerenciamento (antiga conta pagadora). Contas-membro recebem fatura só informativa.

D12. C) Usar o Cost Explorer na conta de gerenciamento com os relatórios de utilização e cobertura de RIs e Savings Plans → revise o capítulo 4

Por quê: Com faturamento consolidado, os descontos de Savings Plans e Reserved Instances são compartilhados entre as contas da organização, e o AWS Cost Explorer na conta de gerenciamento oferece relatórios de utilização e cobertura que mostram como esses descontos estão sendo aplicados. O time financeiro recebe acesso às ferramentas de faturamento, sem permissões administrativas nas contas-membro.

✗ A) Incorreta. AWS Budgets é útil para alertas de custo e uso, mas orçamentos separados por conta não entregam um relatório consolidado de como Savings Plans e RIs estão sendo aplicados;

✗ B) Incorreta. A verificação de otimização de instâncias reservadas do Trusted Advisor recomenda novas compras com base no uso, mas não mostra como os descontos já contratados estão sendo aplicados entre as contas.

✗ D) Incorreta. O Cost Anomaly Detection alerta sobre gastos fora do padrão; não apresenta relatórios de utilização e cobertura de Savings Plans e Reserved Instances.

> **Dica de prova:** Visão centralizada de utilização e cobertura de RIs e Savings Plans em várias contas: Cost Explorer na conta de gerenciamento, com faturamento consolidado.

Agora, treine no formato real

Faça as 6 provas completas do curso CLF-C02: 390 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Amazon Web Services (AWS). As questões são inéditas e não reproduzem a prova real.