PREPARAÇÃO PARA A CERTIFICAÇÃO · CLF-C02

# AWS Certified Cloud Practitioner

Guia de Estudos Completo · 4 domínios da prova

*Renata R Silva (Maki) @renatarsilvax é engenheira de software, criadora de conteúdo tech e 2x certificada AWS (Cloud Practitioner e AI Practitioner). Apaixonada por comunidades, ela compartilha ativamente sua rotina de estudos de engenharia de software e cloud computing nas redes sociais.*

# Introdução

Este guia segue o **guia oficial da prova AWS Certified Cloud Practitioner (CLF-C02)**, domínio por domínio, com tabelas de contraste, palavras-gatilho, armadilhas e um resumo rápido ao final de cada domínio. O conteúdo foi montado a partir de páginas oficiais da AWS (lista completa na seção **Fontes**, ao final).

## Domínios da prova

| Domínio | Peso |
|---|---|
| 1. Conceitos de Nuvem | 24% |
| 2. Segurança e Conformidade | 30% |
| 3. Tecnologia e Serviços de Nuvem | 34% |
| 4. Cobrança, Preços e Suporte | 12% |

## Sobre a prova (guia oficial)

- 65 questões: **50 pontuadas** e 15 não pontuadas (não identificadas), em 90 minutos.
- Tipos: múltipla escolha (1 correta, 3 incorretas) e múltipla resposta (2 ou mais corretas entre 5 ou mais opções).
- Questões sem resposta contam como erradas; **não há penalidade por chute**.
- Resultado: nota escalonada de 100 a 1.000; **nota mínima 700**. Modelo compensatório: você não precisa passar em cada seção, só na prova toda.
- Candidato-alvo: até 6 meses de exposição à nuvem AWS. Fora do escopo: programar, projetar arquitetura, solucionar problemas, implementar e testes de carga.

# Domínio 1: Conceitos de Nuvem (24%)

Tarefas oficiais: 1.1 benefícios da Nuvem AWS · 1.2 princípios de design · 1.3 migração · 1.4 economia da nuvem.

## 1.1 Benefícios da Nuvem AWS

**Computação em nuvem** é o acesso a recursos de TI sob demanda pela internet, pagando apenas pelo que consome. A AWS resume a proposta de valor em **seis vantagens**:

| # | Vantagem | Descrição oficial (resumida) |
|---|---|---|
| 1 | **Trocar despesa fixa por despesa variável** | Em vez de investir pesado em data centers e servidores antes de saber como vai usá-los, você paga só quando consome e só pelo quanto consome. |
| 2 | **Beneficiar-se de economias de escala massivas** | O uso de centenas de milhares de clientes é agregado, o que leva a preços pay-as-you-go menores do que você conseguiria sozinho. |
| 3 | **Parar de adivinhar capacidade** | Evita recursos caros ociosos ou capacidade limitada; escala para cima e para baixo com poucos minutos de aviso. |
| 4 | **Aumentar velocidade e agilidade** | Novos recursos estão a um clique, reduzindo o tempo de disponibilização de semanas para minutos; experimentar custa menos. |
| 5 | **Parar de gastar dinheiro operando e mantendo data centers** | Foco nos clientes e no que diferencia o negócio, e não em instalar, empilhar e energizar servidores. |
| 6 | **Alcance global em minutos** | Implantação em várias Regiões com poucos cliques, com menor latência e melhor experiência para os clientes. |

### Infraestrutura global, alta disponibilidade, elasticidade e agilidade

| Conceito | O que significa |
|---|---|
| Infraestrutura global | Velocidade de implantação e alcance global (Regiões, Zonas de Disponibilidade, locais de borda). Detalhes no Domínio 3. |
| Alta disponibilidade | A aplicação continua operando mesmo com falhas, distribuindo recursos em **várias Zonas de Disponibilidade**. |
| Elasticidade | Capacidade de aumentar e diminuir recursos conforme a demanda (ex.: Amazon EC2 Auto Scaling). |
| Agilidade | Provisionar e experimentar rapidamente, com baixo custo de tentativa e erro. |

**Modelos de serviço e de implantação (conceitos de base).** IaaS: você gerencia SO, aplicação e dados (ex.: Amazon EC2). PaaS: a plataforma é gerenciada, você cuida de aplicação e dados (ex.: AWS Elastic Beanstalk). SaaS: aplicação pronta. Implantação: **nuvem**, **híbrida** (nuvem + on-premises, ex.: AWS Outposts, Direct Connect, VPN) e **on-premises**.

## 1.2 Princípios de design: AWS Well-Architected Framework

O Framework ajuda a entender prós e contras das decisões ao construir sistemas na nuvem, em **seis pilares**. A **AWS Well-Architected Tool** está disponível **sem custo** no AWS Management Console e serve para avaliar cargas de trabalho regularmente, identificar riscos altos e registrar melhorias.

| Pilar | Foco (descrição oficial) | Palavra-gatilho |
|---|---|---|
| **Excelência Operacional** | Executar e monitorar sistemas e melhorar continuamente processos e procedimentos. | operar, monitorar, melhorar processos |
| **Segurança** | Proteger informações e sistemas: confidencialidade dos dados, permissões de usuários, detecção de ameaças. | proteger, permissões |
| **Confiabilidade** | Cargas de trabalho que executam sua função e se recuperam rapidamente de falhas. | recuperar de falhas |
| **Eficiência de Performance** | Alocação estruturada e simplificada de recursos de TI e computação. | usar o recurso certo |
| **Otimização de Custos** | Evitar custos desnecessários: consciência de gastos e dimensionamento correto (rightsizing). | reduzir gastos |
| **Sustentabilidade** | Minimizar os impactos ambientais da execução de cargas de trabalho na nuvem. | impacto ambiental |

**Armadilha:** as perguntas pedem para *diferenciar* os pilares. Identifique a palavra-gatilho do cenário (recuperação, custo, impacto ambiental, permissões) antes de olhar as alternativas.

## 1.3 Migração para a Nuvem AWS

### AWS Cloud Adoption Framework (AWS CAF)

O CAF usa a experiência e as boas práticas da AWS para ajudar na transformação digital. Serve para identificar e priorizar oportunidades, avaliar e melhorar a prontidão para a nuvem (*cloud readiness*) e evoluir o roteiro de forma iterativa. Resultados de negócio citados no guia da prova: **reduzir risco de negócio, melhorar o desempenho ESG, aumentar a receita e aumentar a eficiência operacional**.

| Perspectiva | Foco (descrição oficial) | Stakeholders comuns |
|---|---|---|
| **Negócios** (Business) | Garantir que os investimentos em nuvem acelerem as ambições de transformação digital e os resultados de negócio. | CEO, CFO, COO, CIO, CTO |
| **Pessoas** (People) | Ponte entre tecnologia e negócio: cultura, estrutura organizacional, liderança e força de trabalho. | CIO, COO, CTO, diretor de nuvem |
| **Governança** (Governance) | Orquestrar iniciativas de nuvem maximizando benefícios e minimizando riscos da transformação. | Chief transformation officer, CIO, CTO, CFO, CDO, CRO |
| **Plataforma** (Platform) | Construir plataforma de nuvem híbrida escalável, modernizar cargas e implementar soluções cloud-native. | CTO, líderes de tecnologia, arquitetos, engenheiros |
| **Segurança** (Security) | Confidencialidade, integridade e disponibilidade dos dados e das cargas na nuvem. | CISO, CCO, auditoria interna, arquitetos de segurança |
| **Operações** (Operations) | Garantir que os serviços de nuvem sejam entregues no nível que o negócio precisa. | Líderes de infraestrutura e operações, SREs, gerentes de serviços de TI |

> **Quatro fases iterativas da jornada: Envision** (mostrar como a nuvem acelera resultados de negócio) → **Align** (identificar lacunas de capacidade nas seis perspectivas e alinhar stakeholders) → **Launch** (entregar pilotos em produção) → **Scale** (expandir pilotos e garantir benefícios sustentados).

## As 7 estratégias de migração (7 Rs)

| Estratégia | Definição (AWS Prescriptive Guidance) | Exemplo |
|---|---|---|
| **Retire** | Desativar ou arquivar aplicações; permite desligar os servidores da pilha. | Aplicações "zumbi" (CPU e memória médias abaixo de 5%) ou sem conexão de entrada em 90 dias |
| **Retain** | Manter no ambiente de origem ou ainda não migrar. | Requisito de residência de dados; hardware especializado; recém-atualizada |
| **Rehost** (lift and shift) | Mover para a AWS sem alterar a aplicação. | Pilha de aplicação on-premises para a nuvem, sem mudanças |
| **Relocate** | Transferir muitos servidores de uma vez de uma plataforma on-premises para a versão em nuvem da mesma plataforma, ou mover instâncias/objetos para outra VPC, Região ou conta. Não exige novo hardware nem reescrita. | VMware on-premises para VMware Cloud on AWS; instância RDS para outra VPC ou conta |
| **Repurchase** (drop and shop) | Substituir por outra versão ou produto. | Licença tradicional para SaaS |
| **Replatform** (lift, tinker and shift) | Migrar com alguma otimização para operar com eficiência ou reduzir custo. | Microsoft SQL Server para Amazon RDS for SQL Server |
| **Refactor / Re-architect** | Alterar a arquitetura para aproveitar recursos cloud-native. É a estratégia mais complexa e cara. | Monólito legado redesenhado para a nuvem |

> Em grandes migrações, a AWS recomenda rehost, relocate, replatform e retire, e modernizar (refactor) **depois** da migração.

## Recursos de apoio à migração

| Serviço | Para que serve |
|---|---|
| AWS Migration Hub | Acompanhar o progresso das migrações em um só lugar. |
| AWS Application Discovery Service | Descobrir servidores e aplicações on-premises e suas dependências. |
| AWS Application Migration Service | Rehost automatizado de servidores para a AWS. |
| AWS Database Migration Service (AWS DMS) | Migrar e replicar bancos de dados (inclui **replicação de banco de dados**, citada no guia da prova). |
| AWS Schema Conversion Tool (AWS SCT) | Converter o esquema em migrações entre engines diferentes. |
| Migration Evaluator | Apoiar o caso de negócio e a estimativa da migração. |
| AWS Prescriptive Guidance | Estratégias, guias e padrões de migração. |

## 1.4 Economia da nuvem

| Conceito | Explicação |
|---|---|
| Custo fixo x variável | On-premises envolve custo fixo adiantado (hardware, data center). Na nuvem o custo é variável e proporcional ao uso. |
| Custos associados ao on-premises | Servidores e hardware, espaço, energia e refrigeração, equipe de operação e manutenção, e licenças. |
| Licenciamento | **BYOL** (traga sua própria licença) x **licença incluída** no preço do serviço. AWS License Manager ajuda a gerenciar licenças; Dedicated Hosts permitem usar licenças vinculadas ao servidor. |
| Rightsizing | Ajustar o tamanho dos recursos à carga real. AWS Compute Optimizer e AWS Cost Explorer apoiam a análise. |
| Automação | Infraestrutura como código (AWS CloudFormation) reduz esforço manual e erro humano; processos repetíveis e rápidos. |
| Economias de escala | O volume agregado de clientes reduz o preço por unidade para todos. |

> **Armadilha:** a economia da nuvem não é automática: vem de pagar só pelo uso, rightsizing, desligar recursos ociosos e opções de compra adequadas.

## 1.5 Conceitos de arquitetura que a prova cobra

| Conceito | Definição |
|---|---|
| Escalabilidade vertical (scale up) | Instância maior (mais CPU/RAM). Tem teto e geralmente exige downtime para redimensionar. |
| Escalabilidade horizontal (scale out) | Mais instâncias. Sem teto rígido; combina com balanceadores de carga e com a elasticidade da nuvem. |
| Elasticidade | Crescer **e encolher** automaticamente conforme a demanda; é a propriedade tipicamente "cloud". |
| Alta disponibilidade (HA) | Minimizar downtime, normalmente com recursos redundantes em várias AZs. |
| Tolerância a falhas | O sistema continua funcionando corretamente mesmo quando um componente falha; garantia mais forte que HA. |
| RTO (Recovery Time Objective) | Tempo máximo aceitável para restaurar o serviço (quanto tempo posso ficar fora). |
| RPO (Recovery Point Objective) | Perda máxima de dados aceitável, medida em tempo desde o último backup. |
| Acoplamento fraco (loose coupling) | Componentes se comunicam por interfaces bem definidas (filas, APIs), então a falha de um não se propaga. Serviços: SQS, SNS, EventBridge. |
| Microsserviços x monolito | Microsserviços: aplicação dividida em serviços pequenos e implantáveis de forma independente. Monolito: uma aplicação grande e fortemente acoplada. |

**Padrões de pergunta:** "migrar o mais rápido, com mínimas mudanças" → **Rehost**. "Aproveitar escalabilidade cloud-native a longo prazo, investindo engenharia" → **Refactor**. "Migrar gradualmente conectando o data center à AWS" → **nuvem híbrida** (Direct Connect, Site-to-Site VPN, Storage Gateway, Outposts). "Não ter mais que prever capacidade" → **parar de adivinhar capacidade**. "Passar de investimento inicial para gasto contínuo" → **CapEx para OpEx**.

**Armadilha:** "usar recursos com eficiência e se adaptar à demanda" é **Eficiência de Performance**, não Otimização de Custos; custo é especificamente a dimensão de preço.

## 📋 Resumo rápido do Domínio 1

- 6 vantagens: despesa variável, economia de escala, parar de adivinhar capacidade, velocidade e agilidade, sem custo de data center, alcance global.
- Alta disponibilidade = várias AZs. Elasticidade = escalar para cima e para baixo conforme a demanda.
- Well-Architected: Excelência Operacional, Segurança, Confiabilidade, Eficiência de Performance, Otimização de Custos, Sustentabilidade. Tool é gratuita.
- CAF: Negócios, Pessoas, Governança, Plataforma, Segurança, Operações. Fases: Envision, Align, Launch, Scale.
- 7 Rs: Retire, Retain, Rehost, Relocate, Repurchase, Replatform, Refactor.
- DMS = bancos de dados · Application Migration Service = servidores · Migration Hub = acompanhamento · Discovery Service = inventário.

**Armadilhas:** (1) Rehost não otimiza, apenas move. (2) Relocate não exige reescrever aplicações. (3) Refactor é o mais complexo e caro.

# Domínio 2: Segurança e Conformidade (30%)

Tarefas oficiais: 2.1 modelo de responsabilidade compartilhada · 2.2 conceitos de segurança, governança e conformidade · 2.3 gerenciamento de acesso · 2.4 componentes e recursos de segurança.

## 2.1 Modelo de responsabilidade compartilhada

| | **AWS: segurança *da* nuvem** | **Cliente: segurança *na* nuvem** |
|---|---|---|
| Escopo | Hardware, software, rede e instalações que executam os serviços da AWS. | Dados, aplicações e configuração adequada ao serviço escolhido. |
| Exemplos | Data centers, hardware, infraestrutura global, hypervisor. | Dados, IAM, firewall/security groups, criptografia, SO convidado e patches (no EC2). |

| **Tipo de controle** | **Descrição** | **Exemplos** |
|---|---|---|
| **Herdados** | Totalmente gerenciados pela AWS. | Segurança física e ambiental |
| **Compartilhados** | Ambos contribuem, cada um no seu escopo. | Gerenciamento de patches, gerenciamento de configuração, conscientização e treinamento |
| **Específicos do cliente** | Dependem da implantação do cliente. | Roteamento de dados, segurança de zona |

### Como a responsabilidade muda conforme o serviço

| **Serviço** | **AWS cuida de** | **Você cuida de** |
|---|---|---|
| Amazon EC2 (IaaS) | Hardware e infraestrutura | SO convidado, patches, aplicações, security groups, dados |
| Amazon RDS (gerenciado) | Hardware, SO do host, instalação e patches do engine, backups automatizados | Dados, controle de acesso, configuração de rede e criptografia |
| AWS Lambda (serverless) | Infraestrutura, SO e runtime | Seu código, permissões IAM e dados |
| Amazon S3 / DynamoDB | Operação da infraestrutura | Classificação de dados e permissões IAM |

> **Armadilha:** quanto mais gerenciado o serviço, menor a responsabilidade do cliente; mas dados e acessos são **sempre** do cliente.

## 2.2 Segurança, governança e conformidade

### Conformidade

- **AWS Artifact:** portal de autoatendimento para baixar relatórios de conformidade da AWS e aceitar acordos. É onde encontrar informações de conformidade.
- Requisitos de conformidade variam por **localização geográfica**, **setor** e **serviço**; consulte a página AWS Compliance.

### Criptografia

| Tipo | Protege | Ferramentas |
|---|---|---|
| Em trânsito | Dados movendo-se pela rede (TLS/HTTPS) | AWS Certificate Manager (ACM), VPN |
| Em repouso | Dados armazenados | AWS KMS (chaves), AWS CloudHSM (HSM dedicado), criptografia nativa de S3, EBS, RDS |

### Monitoramento, auditoria e logs

| Serviço | Função | Pergunta que responde |
|---|---|---|
| **Amazon CloudWatch** | Monitoramento: métricas, logs e alarmes | Como está o desempenho? |
| **AWS CloudTrail** | Registra chamadas de API e atividade na conta | Quem fez o quê, quando? |
| **AWS Config** | Avalia e registra configurações dos recursos e conformidade | Como o recurso está configurado e mudou? |
| **Relatórios de acesso** | IAM credential report e informações de último acesso | Quais credenciais e permissões estão sem uso? |

## Serviços para proteger recursos

| Serviço | Para que serve |
|---|---|
| **Amazon GuardDuty** | Detecção inteligente de ameaças nas contas e cargas de trabalho. |
| **Amazon Inspector** | Varredura automatizada de vulnerabilidades (ex.: EC2, imagens de contêiner, Lambda). |
| **AWS Security Hub** | Visão centralizada de alertas e achados de segurança e verificações de conformidade. |
| **AWS Shield** | Proteção contra DDoS. **Standard**: automático, gratuito, para todos os clientes. **Advanced**: pago, detecção e mitigação mais sofisticadas, acesso 24/7 a equipe de resposta a DDoS e proteção de custos. |
| **AWS WAF** | Firewall de aplicações web: protege contra exploits web comuns. |
| **AWS Firewall Manager** | Gerenciar centralmente regras de firewall (ex.: WAF) em várias contas via AWS Organizations. |
| **Amazon Macie** | Descobrir e proteger dados sensíveis, como PII, no Amazon S3. |
| **Amazon Detective** | Investigar a causa raiz de achados de segurança. |
| **AWS KMS** | Criar e controlar chaves de criptografia. |
| **AWS CloudHSM** | Módulo de segurança de hardware dedicado. |
| **AWS Secrets Manager** | Armazenar e rotacionar segredos (senhas, chaves de API). |
| **AWS Certificate Manager** | Provisionar e gerenciar certificados SSL/TLS. |
| **AWS Resource Access Manager** | Compartilhar recursos entre contas com segurança. |
| **Amazon Cognito** | Identidade e acesso para clientes de aplicações web e mobile. |
| **AWS Directory Service** | Microsoft Active Directory gerenciado. |
| **AWS Audit Manager** | Auditar continuamente o uso da AWS para simplificar a avaliação de risco e conformidade (citado em material de estudo; não consta na lista oficial de serviços da prova). |

## 2.3 Gerenciamento de acesso

| Conceito | Descrição |
|---|---|
| **AWS IAM** | Controla quem (autenticação) pode fazer o quê (autorização) nos recursos. |
| Usuários, grupos, roles | Usuário = identidade de pessoa ou aplicação; grupo = conjunto de usuários; role = identidade com credenciais temporárias, assumida por pessoas, serviços ou outras contas. |
| Políticas | Documentos JSON que definem permissões. **Gerenciadas pela AWS** (prontas) ou **gerenciadas pelo cliente** (customizadas); também há políticas inline. |
| **Menor privilégio** | Conceder apenas as permissões necessárias para a tarefa. |
| **MFA** | Segundo fator de autenticação; recomendada para root e usuários IAM. |
| **IAM Identity Center** | Gerenciamento centralizado de acesso da força de trabalho a várias contas e aplicações (identidade federada). |
| Funções entre contas | Roles IAM permitem acesso entre contas (cross-account). |
| Chaves de acesso | Credenciais de longo prazo; prefira credenciais temporárias via roles e atualize as chaves quando necessário. |
| Armazenar credenciais | AWS Secrets Manager e AWS Systems Manager (Parameter Store). |

### Usuário root

- Identidade inicial com acesso total à conta. **Não use para tarefas do dia a dia**; use um usuário administrativo no IAM Identity Center.
- Proteja com **MFA**, senha forte e remova chaves de acesso do root quando não forem necessárias.
- **Tarefas que exigem o root** (lista oficial, trechos): alterar configurações da conta (e-mail, senha) em contas autônomas; fechar a conta; reabrir a conta; restaurar permissões de IAM quando o único administrador revogou as próprias; ativar o acesso do IAM ao console de Billing; cadastrar-se no AWS GovCloud (US); registrar-se como vendedor no mercado de Reserved Instances do EC2; configurar MFA delete em bucket do S3; editar ou excluir política de bucket S3 ou de fila SQS que nega todos os principais.

### Boas práticas oficiais de IAM

- Exigir federação com um provedor de identidade e credenciais temporárias para pessoas.
- Exigir que cargas de trabalho usem roles IAM (credenciais temporárias).
- Exigir MFA (preferir MFA resistente a phishing, como passkeys e chaves de segurança).
- Aplicar permissões de menor privilégio; começar por políticas gerenciadas da AWS e evoluir para as do cliente.
- Usar o IAM Access Analyzer para validar políticas e verificar acesso público ou entre contas.
- Revisar e remover usuários, roles, permissões e credenciais sem uso.
- Usar SCPs do AWS Organizations como guardrails (eles não concedem permissões) e permissions boundaries para delegar.

## 2.4 Componentes e recursos de segurança

- **Third-party:** produtos de segurança de terceiros estão disponíveis no **AWS Marketplace**.
- **Onde achar informações:** AWS Knowledge Center, AWS Security Center e AWS Security Blog.
- **AWS Trusted Advisor:** verifica o ambiente e recomenda ações em custo, performance, segurança, resiliência, excelência operacional e limites de serviço. (Material mais antigo cita 5 categorias: custo, performance, segurança, tolerância a falhas e limites de serviço.)

## 2.5 Segurança de rede e quadros-resumo

| | **Security Group** | **Network ACL (NACL)** |
|---|---|---|
| Nível | Instância (EC2/ENI) | Sub-rede |
| Estado | **Stateful**: o tráfego de resposta é permitido automaticamente | **Stateless**: regras de entrada e saída precisam ser definidas |
| Tipos de regra | Apenas permitir | Permitir e negar |
| Avaliação | Todas as regras são avaliadas | Em ordem numérica; a primeira correspondência vale |

| **Componente** | **Função** |
|---|---|
| Sub-redes, tabelas de rota, Internet Gateway | Sub-rede pública tem rota para a internet por meio do Internet Gateway. |
| NAT Gateway | Permite saída para a internet a partir de sub-redes privadas, sem permitir entrada. |
| VPC Peering | Conexão direta entre duas VPCs. |
| VPC Endpoints | Acesso privado da VPC a serviços da AWS sem passar pela internet pública. |

## Qual serviço usar? (tabela de gatilhos)

| Necessidade | Resposta |
|---|---|
| Acesso temporário de um serviço AWS a outro (ex.: EC2 acessar S3) | **IAM Role** (nunca chaves fixas na instância) |
| Alguém de outra conta precisa acessar seus recursos | Role IAM entre contas |
| Login centralizado em várias contas | IAM Identity Center |
| Segurança extra no login | MFA |
| Menor privilégio para novo funcionário | Política IAM customizada anexada a um grupo |
| Configuração está em conformidade? O que mudou? | AWS Config |
| Quem fez qual chamada de API e quando? | AWS CloudTrail |
| Dados sensíveis/PII no S3 | Amazon Macie |
| Instância comprometida ou atividade maliciosa | Amazon GuardDuty (analisa CloudTrail, VPC Flow Logs e logs de DNS) |
| Vulnerabilidades (CVEs) em EC2, contêineres, Lambda | Amazon Inspector |
| Painel único de achados de segurança | AWS Security Hub |
| SQL injection e XSS na aplicação web | AWS WAF (camada 7; CloudFront, ALB, API Gateway) |
| DDoS | AWS Shield |
| Regras de WAF/security groups em várias contas | AWS Firewall Manager |
| Certificados de conformidade da AWS (SOC, PCI-DSS, ISO) e acordos (ex.: BAA) | AWS Artifact |
| Guardar e rotacionar senha de banco de dados | AWS Secrets Manager |
| Gerenciar chaves de criptografia | AWS KMS (chaves gerenciadas pela AWS ou pelo cliente) |
| Certificado SSL/TLS gratuito para o load balancer | AWS Certificate Manager |
| Verificação de boas práticas em custo/segurança/performance | AWS Trusted Advisor |

> **Config x CloudTrail** é o par mais confundido do domínio: **Config** = como o recurso está e como mudou; **CloudTrail** = quem fez o quê, quando e de onde.

## 📋 Resumo rápido do Domínio 2

- AWS = segurança *da* nuvem. Cliente = segurança *na* nuvem.
- Patches, configuração e treinamento = controles compartilhados.
- AWS Artifact = relatórios de conformidade. CloudTrail = quem chamou a API. CloudWatch = métricas e logs. Config = configuração e conformidade.
- GuardDuty = ameaças · Inspector = vulnerabilidades · Macie = dados sensíveis no S3 · Shield = DDoS · WAF = ataques web · Security Hub = visão central.
- KMS = chaves · CloudHSM = HSM dedicado · Secrets Manager = segredos · ACM = certificados.
- Root: MFA e uso mínimo. Dia a dia: IAM Identity Center. Menor privilégio sempre.

> **Armadilhas:** (1) Dados e IAM sempre são do cliente. (2) CloudTrail (auditoria de API) não é o mesmo que CloudWatch (monitoramento). (3) SCPs não concedem permissões.

# Domínio 3: Tecnologia e Serviços de Nuvem (34%)

Tarefas oficiais: 3.1 implantar e operar · 3.2 infraestrutura global · 3.3 computação · 3.4 bancos de dados · 3.5 rede · 3.6 armazenamento · 3.7 IA/ML e análise de dados · 3.8 outras categorias.

## 3.1 Métodos de implantação e operação

| Método | Quando usar |
|---|---|
| **AWS Management Console** | Interface web; ideal para operações pontuais e exploração. |
| **AWS CLI** | Linha de comando; automação e scripts. |
| **SDKs e APIs** | Acesso programático a partir do código da aplicação. |
| **Infraestrutura como código (IaC)** | Processos **repetíveis** e versionados (ex.: AWS CloudFormation). |

> Operação **pontual** → Console. Processo **repetível** → CLI/SDK/IaC. Modelos de implantação: **nuvem**, **híbrido**, **on-premises**.

## 3.2 Infraestrutura global da AWS

| Componente | Definição |
|---|---|
| **Região** | Localização física onde a AWS agrupa data centers; cada Região tem no **mínimo três** AZs isoladas e fisicamente separadas. |
| **Zona de Disponibilidade (AZ)** | Um ou mais data centers discretos com energia, rede e conectividade redundantes; AZs ficam a muitos quilômetros uma da outra, dentro de 100 km, ligadas por rede de baixa latência. |
| **Locais de borda** | Pontos de presença usados para entregar conteúdo com baixa latência (ex.: Amazon CloudFront). |
| **Local Zones** | Extensões de uma Região que colocam computação e armazenamento mais perto dos usuários (latência de milissegundos de um dígito). |
| **AWS Wavelength** | Infraestrutura embutida em redes 5G de operadoras para aplicações de latência ultrabaixa. |

- **Alta disponibilidade:** distribuir a carga em **várias AZs**; AZs não compartilham pontos únicos de falha.
- **Quando usar várias Regiões:** recuperação de desastres, continuidade de negócios, baixa latência para usuários finais e **soberania de dados**.
- Na consulta à página oficial: 39 Regiões e 124 AZs (os números mudam com o tempo).

## 3.3 Serviços de computação

| Família de instância EC2 | Uso |
|---|---|
| Uso geral | Equilíbrio de computação, memória e rede (servidores web, bancos de dados). |
| Otimizada para computação | Aplicações intensivas em processador (processamento em lote, transcodificação de mídia, servidores de jogos). |
| Otimizada para memória | Grandes conjuntos de dados em RAM (bancos em memória, análise). |
| Computação acelerada | Aceleradores de hardware (gráficos, ML). |
| Otimizada para armazenamento | Milhões de operações de E/S aleatórias de baixa latência (bancos de alto throughput). |
| Otimizada para HPC | Melhor custo-benefício para cargas de HPC em escala. |

| Serviço | Descrição |
|---|---|
| **Amazon EC2** | Capacidade de computação segura e redimensionável (servidores virtuais). |
| **EC2 Auto Scaling** | Adiciona ou remove instâncias conforme condições definidas: dá **elasticidade**. |
| **Elastic Load Balancing** | Distribui o tráfego entre vários destinos. **ALB**: HTTP/HTTPS (camada 7). **NLB**: TCP, desempenho extremo (camada 4). **GWLB**: appliances de terceiros. |
| **AWS Lambda** | Executa código sem gerenciar servidores; paga só pelo tempo de computação. |
| **AWS Fargate** | Motor serverless para contêineres (ECS e EKS), sem gerenciar servidores. |
| **Amazon ECS** | Orquestração de contêineres, simples e nativa da AWS. **Amazon EKS**: Kubernetes gerenciado (quando precisa especificamente de Kubernetes ou estratégia portável). **Amazon ECR**: registro de imagens. |
| **AWS Elastic Beanstalk** | Você envia o código; o serviço cuida de provisionamento, balanceamento, escala e monitoramento. |
| **Amazon Lightsail** | Servidor privado virtual simples, com preço baixo e previsível. |
| **AWS Batch** | Processamento em lote em qualquer escala. |
| **AWS Outposts** | Infraestrutura e serviços da AWS no seu data center (híbrido). |

## 3.4 Serviços de banco de dados

| Tipo | Serviço | Observação oficial |
|---|---|---|
| Relacional | **Amazon RDS** | Configura, opera e escala bancos relacionais; automatiza provisionamento, patches e backups. |
| Relacional | **Amazon Aurora** | Compatível com MySQL e PostgreSQL; replicação em três AZs; gerenciado pelo RDS. |
| Chave-valor / NoSQL | **Amazon DynamoDB** | Chave-valor e documentos; desempenho de milissegundos de um dígito em qualquer escala. |
| Em memória | **Amazon ElastiCache** | Cache em memória (Redis OSS e Memcached) para acelerar aplicações. |
| Documentos | **Amazon DocumentDB** | Compatível com MongoDB. |
| Grafo | **Amazon Neptune** | Dados altamente conectados: detecção de fraude, recomendações. |
| Data warehouse | **Amazon Redshift** | Armazenamento de dados analítico com SQL. |

- **EC2 x banco gerenciado:** no EC2 você administra tudo (SO, patches, backups); com serviços gerenciados a AWS assume essas tarefas.
- **Migração:** AWS DMS (migração e replicação) e AWS SCT (conversão de esquema).

## 3.5 Serviços de rede

| Serviço / componente | Descrição |
|---|---|
| **Amazon VPC** | Seção logicamente isolada da nuvem, com controle do intervalo de IPs, sub-redes, tabelas de rota e gateways. |
| Sub-rede pública x privada | Pública tem acesso à internet; privada abriga backends sem acesso direto à internet. |
| **Security groups** | Firewall no nível da instância (permitem tráfego; **stateful**). |
| **Network ACLs** | Firewall no nível da sub-rede (**stateless**, regras de permitir e negar). |
| **Amazon Route 53** | DNS altamente disponível e escalável; roteamento por latência, geolocalização, ponderado e failover; registro de domínios. |
| **Amazon CloudFront** | CDN que entrega conteúdo globalmente com baixa latência. |
| **AWS Direct Connect** | Conexão de rede **dedicada** entre o seu local e a AWS. |
| **AWS Site-to-Site VPN / Client VPN** | Túneis criptografados entre redes e a AWS; Client VPN para usuários remotos. |
| **AWS Transit Gateway** | Hub central que conecta VPCs e redes on-premises (modelo hub-and-spoke). |
| **AWS PrivateLink** | Conectividade privada entre VPCs, serviços AWS e aplicações on-premises, sem expor à internet. |
| **AWS Global Accelerator** | Usa a rede global da AWS e IPs estáticos para melhorar disponibilidade e desempenho. |
| **Amazon API Gateway** | Cria, publica e protege APIs em qualquer escala. |

> **Armadilha:** Direct Connect = conexão dedicada e privada; VPN = túnel criptografado pela internet. Amazon Inspector não é firewall; segurança de rede na VPC é feita com security groups e NACLs.

## 3.6 Serviços de armazenamento

| Tipo | Serviço | Descrição |
|---|---|---|
| Objetos | **Amazon S3** | Escalabilidade, disponibilidade e durabilidade de 99,999999999% (11 noves). |
| Blocos | **Amazon EBS** | Volumes persistentes para EC2, replicados dentro da AZ. **Instance store**: armazenamento temporário local da instância. |
| Arquivos | **Amazon EFS** | Sistema de arquivos elástico para Linux, compartilhado por milhares de instâncias. |
| Arquivos | **Amazon FSx** | Sistemas de arquivos gerenciados (Windows File Server, Lustre, NetApp ONTAP, OpenZFS). |
| Híbrido | **AWS Storage Gateway** | Aplicações on-premises usam o armazenamento da AWS, com cache local. |
| Proteção | **AWS Backup** | Centraliza e automatiza backups em vários serviços (políticas, integração com Organizations). |
| Recuperação | **AWS Elastic Disaster Recovery** | Recuperação rápida de aplicações on-premises e na nuvem. |

### Classes de armazenamento do Amazon S3

| Classe | Uso |
|---|---|
| S3 Standard | Dados acessados com frequência. |
| S3 Intelligent-Tiering | Padrão de acesso desconhecido ou variável; move objetos entre camadas automaticamente. |
| S3 Express One Zone | Acesso de alto desempenho, latência de milissegundos de um dígito, em uma AZ. |
| S3 Standard-IA | Acesso infrequente; várias AZs. |
| S3 One Zone-IA | Acesso infrequente; uma única AZ (custa menos). |
| S3 Glacier Instant Retrieval | Arquivo acessado poucas vezes por ano, com recuperação imediata. |
| S3 Glacier Flexible Retrieval | Backup e arquivo; recuperação de minutos a horas. |
| S3 Glacier Deep Archive | Menor custo; recuperação em 12 a 48 horas; retenção longa. |

- **Políticas de ciclo de vida:** movem objetos automaticamente entre classes (ou os expiram) sem mudar a aplicação.
- S3 Object Lock: armazenamento WORM (escreve uma vez, lê várias).

## 3.7 IA/ML e análise de dados

| Serviço | O que faz |
|---|---|
| **Amazon SageMaker AI** | Construir, treinar e implantar modelos de ML. |
| **Amazon Lex** | Chatbots conversacionais (voz e texto). |
| **Amazon Comprehend** | Processamento de linguagem natural: sentimento, entidades, frases-chave. |
| **Amazon Rekognition** | Análise de imagens e vídeos. |
| **Amazon Textract** | Extração de texto e dados de documentos. |
| **Amazon Transcribe** | Fala para texto. |
| **Amazon Polly** | Texto para fala. |
| **Amazon Translate** | Tradução de idiomas. |
| **Amazon Q** | Assistente de IA generativa. |

| Serviço de análise | Descrição oficial |
|---|---|
| **Amazon Athena** | Consultas SQL interativas sobre dados no S3; serverless, paga por consulta. |
| **Amazon Kinesis** | Coletar, processar e analisar dados de streaming em tempo real. |
| **AWS Glue** | Serviço ETL totalmente gerenciado; mantém o Data Catalog. |
| **Amazon Quick** | Business intelligence na nuvem: dashboards interativos. |
| **Amazon EMR** | Plataforma de big data com Spark, Hive, Presto e outros. |
| **Amazon Redshift** | Data warehouse na nuvem. |
| **Amazon OpenSearch Service** | Busca, análise de logs e visualização. |

## 3.8 Outras categorias de serviço

| Categoria | Serviços e função |
|---|---|
| Integração de aplicações | **Amazon SQS**: filas (desacopla; padrão = ordem best-effort, FIFO = ordem garantida). **Amazon SNS**: pub/sub, notificações push, e-mail e SMS. **Amazon EventBridge**: barramento de eventos serverless. **AWS Step Functions**: fluxos visuais. |
| Aplicações de negócio | **Amazon Connect**: central de contato. **Amazon SES**: envio de e-mail. |
| Ferramentas de desenvolvedor | **AWS CodeBuild**: compila e testa. **AWS CodePipeline**: pipeline de entrega contínua. **AWS X-Ray**: rastreia e depura aplicações. **AWS CLI**. |
| Computação do usuário final | **Amazon AppStream 2.0**: transmite aplicações. **Amazon WorkSpaces**: desktops virtuais. **WorkSpaces Secure Browser**: navegador seguro. |
| Frontend web e mobile | **AWS Amplify**: criar e implantar apps web e mobile. |
| IoT | **AWS IoT Core**: conectar e gerenciar dispositivos IoT. |
| Suporte ao cliente | **AWS Support**: opções de assistência técnica (ver Domínio 4). |

## 3.9 Comparativos e dicas de prova

| Par | Diferença |
|---|---|
| CloudFormation x Elastic Beanstalk | CloudFormation: define cada recurso em modelos JSON/YAML (controle total, repetível, versionável, "stack"). Beanstalk: envie o código e ele provisiona tudo (menos controle, mais rápido). AWS CDK: IaC em linguagens de programação, gera CloudFormation (não consta na lista oficial). |
| CloudFront x Global Accelerator | CloudFront: cache na borda, ideal para conteúdo estático/cacheável. Global Accelerator: roteia tráfego pela rede da AWS, ideal para tráfego dinâmico, TCP/UDP (jogos, VoIP). |
| SQS x SNS | SQS: fila, pull, uma mensagem consumida por um consumidor. SNS: tópico, push, fan-out para vários assinantes (e-mail, SMS, Lambda, SQS). |
| EBS x EFS x S3 | EBS: bloco, uma instância por vez (disco virtual). EFS: arquivo (NFS), várias instâncias ao mesmo tempo. S3: objeto, via API, sem "montar" no servidor. |
| RDS/Aurora x DynamoDB | Relacional/SQL/estruturado x NoSQL, escala massiva, esquema flexível. |
| Direct Connect x VPN | Linha privada dedicada, banda consistente x túnel criptografado pela internet, mais rápido de configurar. |

- **Spot:** pode ser interrompido com aviso de 2 minutos; nunca para cargas críticas ou stateful.
- **S3 recursos:** versionamento (protege contra exclusão/sobrescrita acidental), políticas de ciclo de vida, replicação entre Regiões ou na mesma Região, criptografia e Block Public Access.
- **AWS Snow Family** (Snowcone, Snowball, Snowmobile): transferência física de grandes volumes de dados quando há pouca ou nenhuma banda.

- **AWS Systems Manager:** hub operacional: patches, comandos em frotas, Parameter Store, Session Manager (shell sem SSH).
- **AWS Organizations:** gerencia várias contas, com faturamento consolidado e **SCPs** (limite máximo de permissões; são guardrails, não concedem permissões). **AWS Control Tower** cria um ambiente multi-conta (landing zone) com boas práticas.
- **CI/CD:** CodeBuild (compila) e CodePipeline (orquestra) estão no escopo oficial; CodeCommit e CodeDeploy aparecem em material de estudo, mas não constam na lista oficial atual.
- **Fora da lista oficial, mas citados em material de estudo:** Amazon Kendra (busca corporativa) e Amazon Bedrock (modelos de fundação por API).

## 📋 Resumo rápido do Domínio 3

- Região ≥ 3 AZs. Alta disponibilidade = várias AZs. Várias Regiões = DR, baixa latência, soberania de dados.
- EC2 (VMs), Lambda (serverless), Fargate (contêineres serverless), ECS/EKS (contêineres), Beanstalk (PaaS), Lightsail (simples), Outposts (híbrido).
- RDS/Aurora = relacional · DynamoDB = NoSQL · ElastiCache = memória · Neptune = grafo · DocumentDB = documentos · Redshift = data warehouse.
- Security group = instância (stateful). NACL = sub-rede (stateless). Direct Connect = dedicado. VPN = criptografado pela internet.
- S3 = objetos · EBS = blocos · EFS/FSx = arquivos · Storage Gateway = híbrido · Backup = backups centralizados.
- Athena = SQL no S3 · Glue = ETL · Kinesis = streaming · Quick = BI · SageMaker AI = ML · Lex = chatbot.
- SQS = fila · SNS = notificação · EventBridge = eventos.

> **Armadilhas:** (1) EBS é bloco; EFS é arquivo; S3 é objeto. (2) Aurora é gerenciado pelo RDS. (3) Glacier Deep Archive leva horas para recuperar.

# Domínio 4: Cobrança, Preços e Suporte (12%)

Tarefas oficiais: 4.1 modelos de preços · 4.2 faturamento, orçamento e gestão de custos · 4.3 recursos técnicos e planos de suporte.

## 4.1 Modelos de preços

Princípios oficiais: **pague conforme o uso**; **economize ao se comprometer** (Savings Plans, em US$/hora por 1 ou 3 anos); **pague menos usando mais** (preço em camadas por volume).

| Opção de compra | Descrição | Quando usar |
|---|---|---|
| **On-Demand** | Paga por hora ou segundo, sem compromisso nem pagamento adiantado. | Cargas curtas, imprevisíveis, que não podem ser interrompidas; primeiros testes. |
| **Savings Plans** | Preço menor (até 72%) em troca do compromisso de uso consistente (US$/hora) por 1 ou 3 anos. | Uso estável e flexível. |
| **Reserved Instances** | Desconto de até 72% sobre On-Demand. Convertible RIs permitem trocar família, SO e tenancy. | Uso previsível e contínuo. |
| **Spot Instances** | Capacidade ociosa com até 90% de desconto. | Cargas tolerantes a falhas, com início e fim flexíveis. |
| **Dedicated Hosts** | Servidor físico dedicado a você; permite licenças vinculadas ao servidor (ex.: Windows Server, SQL Server). | Licenciamento e conformidade. |
| **Dedicated Instances** | Instâncias em hardware dedicado a um único cliente. | Isolamento de hardware. |
| **Capacity Reservations** | Reserva de capacidade para disponibilidade garantida em eventos críticos ou recuperação de desastres. | Garantir capacidade. |

- **Reserved Instances no AWS Organizations:** com o faturamento consolidado, os descontos de RI e Savings Plans podem ser compartilhados entre as contas.
- **Cobrança por segundo** (mínimo de 60 segundos) nas instâncias EC2.

### Transferência de dados e armazenamento

- Transferência de dados **de entrada (IN) é gratuita**; a de **saída (OUT)** é cobrada em camadas, com preço menor conforme o volume.
- Transferência entre Regiões tem custo; o preço do armazenamento varia por serviço e por camada/classe (ex.: classes do S3).
- O nível gratuito (Free Tier) permite experimentar serviços.

## 4.2 Faturamento, orçamento e gestão de custos

| Ferramenta | Função |
|---|---|
| **AWS Pricing Calculator** | Estima o custo de uma arquitetura **antes** de implantar. |
| **AWS Cost Explorer** | Visualiza, entende e gerencia custos e uso ao longo do tempo; permite previsão. |
| **AWS Budgets** | Define limites e envia alertas quando o gasto real ou previsto excede o orçamento. |
| **AWS Cost and Usage Report** | Dados detalhados de custo e uso, o mais abrangente. |
| **AWS Billing Conductor** | Estratégia de alocação de custos alinhada à lógica do negócio. |
| **AWS Compute Optimizer** | Recomendações para rightsizing de computação. |

### AWS Organizations e faturamento consolidado

- Há uma conta de **gerenciamento** que paga as cobranças de todas as contas-membro.
- Benefícios: **uma única fatura**, rastreamento fácil, **uso combinado** (descontos por volume, de RIs e de Savings Plans compartilhados) e **sem custo adicional**.

### Tags de alocação de custos

- Rótulos chave-valor aplicados a recursos. Dois tipos: **geradas pela AWS** (prefixo `aws:`) e **definidas pelo usuário** (prefixo `user:`).
- Precisam ser **ativadas** no console de Billing e levar até 24 horas para aparecer; ficam disponíveis no Cost Explorer e nos relatórios (ex.: Cost and Usage Report).

## 4.3 Recursos técnicos e planos de suporte

| Plano | Destaques (página oficial dos planos) |
|---|---|
| **Basic Support** | Incluído para todos: atendimento ao cliente 24/7, documentação, whitepapers, AWS re:Post, verificações centrais do Trusted Advisor e AWS Health. |
| **Business Support+** | Mínimo recomendado para cargas de produção: resposta em menos de 30 min (sistema crítico fora) e 1 hora (produção fora); suporte 24/7 por telefone, web, chat e e-mail; suporte de conta e cobrança; verificações completas do Trusted Advisor. |
| **Enterprise Support** | Cargas críticas: resposta em menos de 15 min; **Technical Account Manager (TAM)** designado; plano estratégico personalizado; revisões proativas de segurança. |
| **Unified Operations** | Cargas de missão crítica: resposta em menos de 5 min por Incident Management Engineer; Domain Specialist Engineers; revisões arquiteturais contínuas. |

> **AWS Trusted Advisor** recomenda ações em seis áreas: custo, performance, segurança, resiliência, excelência operacional e limites de serviço. Todas as contas têm 56 verificações fundamentais; Business Support+ ou superior libera o conjunto ampliado (482 verificações, segundo a página oficial), com acesso por API e CLI.

| Recurso | Para que serve |
|---|---|
| AWS Health Dashboard / AWS Health API | Eventos de saúde dos serviços e da sua conta; acompanhar e gerenciar o ambiente. |
| AWS Knowledge Center, AWS re:Post, AWS Prescriptive Guidance | Perguntas frequentes, comunidade e orientação técnica. |
| Whitepapers, blogs e documentação | Material oficial nos sites da AWS. |
| AWS Support Center | Abrir e acompanhar casos de suporte. |
| AWS Trust and Safety | Relatar abuso de recursos da AWS. |
| AWS Professional Services e solutions architects | Assistência técnica da AWS. |
| AWS Partner Network (APN) | Parceiros, incluindo ISVs e integradores de sistemas; benefícios como treinamento e certificação, eventos e descontos por volume. |
| AWS Marketplace | Catálogo digital de software de terceiros, com ferramentas de gestão de custos, governança e direitos de uso. |

### Nível gratuito (Free Tier) e outros itens

- **Always Free:** gratuito para sempre até um limite (ex.: primeiro milhão de requisições do Lambda por mês).
- **12 meses gratuitos:** a partir da criação da conta, até limites de uso.
- **Trials:** testes de curto prazo a partir da ativação do serviço (varia por serviço).
- **AWS Marketplace:** software de terceiros (AMIs, SaaS, dados) implantado na sua conta e cobrado na fatura AWS.
- **Migration Evaluator:** constrói o caso de negócio e a estimativa de custo da migração; **Application Discovery Service** coleta dados de servidores on-premises.
- **Recomendações do Cost Explorer** mostram onde comprometer (RIs/Savings Plans) economizaria, com base no histórico de uso.

> **Atenção a planos antigos:** materiais de estudo mais antigos citam os planos **Developer**, **Business** e **Enterprise On-Ramp**. A página oficial atual e o guia da prova listam Basic, Business Support+, Enterprise Support e Unified Operations. Se um simulado usar os nomes antigos, trate-os como versão anterior. Em qualquer versão, só o Basic é gratuito e o TAM só vem nos planos de nível Enterprise.

## 📋 Resumo rápido do Domínio 4

- On-Demand = flexível · Savings Plans/RIs = compromisso (até 72%) · Spot = até 90%, pode ser interrompido · Dedicated Hosts = licenças e conformidade.
- Dados IN são gratuitos; dados OUT são cobrados em camadas.
- Pricing Calculator = estimar antes · Cost Explorer = analisar o passado e prever · Budgets = alertas · CUR = relatório detalhado.
- Organizations = fatura única e descontos combinados, sem custo. Tags precisam ser ativadas.
- Planos: Basic, Business Support+, Enterprise Support, Unified Operations. TAM no Enterprise Support.
- Trusted Advisor = recomendações; Health Dashboard = eventos de serviço.

> **Armadilhas:** (1) Spot pode ser interrompido. (2) Pricing Calculator estima; Cost Explorer analisa gastos reais. (3) Tags não aparecem sem ativação.

# Revisão Final

## Tabela de contrastes (revisão de última hora)

| Par confundível | Distinção |
|---|---|
| Escalabilidade x Elasticidade | Escalabilidade: pode crescer. Elasticidade: cresce e encolhe automaticamente. |
| HA x Tolerância a falhas | HA: minimiza downtime com redundância. Tolerância a falhas: continua funcionando durante a falha. |
| RTO x RPO | RTO: tempo para recuperar. RPO: perda de dados aceitável (tempo desde o último backup). |
| Vertical x Horizontal | Vertical: instância maior, com teto. Horizontal: mais instâncias, sem teto rígido. |
| Security Group x NACL | Instância, stateful, só permite x sub-rede, stateless, permite e nega, em ordem. |
| Config x CloudTrail | Configuração/conformidade x quem chamou qual API. |
| CloudFront x Global Accelerator | Cache na borda x roteamento otimizado de tráfego dinâmico. |
| SQS x SNS | Fila, pull, um consumidor x tópico, push, vários assinantes. |
| EBS x EFS x S3 | Bloco x arquivo compartilhado x objeto. |
| Direct Connect x VPN | Dedicado e privado x criptografado pela internet. |
| CapEx x OpEx | Investimento inicial x gasto conforme o uso. |
| RIs x Savings Plans | Compromisso com instância específica x compromisso em US$/hora, mais flexível. |
| Cost Explorer x Pricing Calculator | Gastos reais passados x estimativa futura. |
| IAM Role x IAM User | Temporária, assumida x identidade persistente. |
| GuardDuty x Inspector x Security Hub | Ameaças a partir de logs x vulnerabilidades/CVEs x painel agregado. |

## Armadilhas que custam pontos

1. "A AWS cuida disso automaticamente" é errado para desenho de IAM, escolha de chaves de criptografia, regras de security group e patches do SO em EC2.
2. Security Group x NACL: leia "instância" x "sub-rede" e "stateful" x "regras nos dois sentidos".
3. Spot nunca é a resposta para carga que não tolera interrupção ou é crítica/stateful.
4. CloudFront (estático/cacheável) x Global Accelerator (dinâmico, jogos, VoIP).
5. Config x CloudTrail: "como o recurso está" x "quem chamou qual API".
6. Planos de suporte: só o Basic é gratuito; não misture os tempos de resposta (Business Support+ x Enterprise Support).

7. RTO é tempo; RPO é dados. Não troque.
8. Migração "mais rápida e barata para começar" é Rehost, não Refactor.
9. SCPs são guardrails, não concedem permissões; as políticas IAM da conta ainda precisam permitir.
10. "Como reduzir custos" tem várias respostas possíveis: combine a palavra-chave (uso estável, interrompível, dados que envelhecem) com a ferramenta (RI/Savings Plans, Spot, ciclo de vida do S3).

## Autoteste: explique em voz alta

1. Qual a diferença entre elasticidade e escalabilidade?
2. Por que o security group é stateful e a NACL não? O que isso muda para o pacote de resposta?
3. Dê um cenário em que Spot é ideal e outro em que é perigoso.
4. O que o AWS Config registra e o que o CloudTrail registra?
5. No modelo de responsabilidade compartilhada, cite três coisas que continuam sendo do cliente mesmo no RDS.
6. Por que escolher Global Accelerator em vez de CloudFront para um jogo multiplayer em tempo real?
7. Qual a diferença entre RTO e RPO e como cada um aparece num requisito de recuperação de desastres?
8. Quando escolher DynamoDB em vez de RDS?
9. Qual a diferença em uma frase entre SQS e SNS?
10. Qual plano de suporte inclui um Technical Account Manager e o que ele faz que um chamado comum não faz?

# Fontes

Conteúdo consultado em **21/11/2026**, em páginas públicas do **site oficial da AWS** (aws.amazon.com e docs.aws.amazon.com):

- Guia oficial da prova CLF-C02: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02.html
- Domínio 1: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain1.html
- Domínio 2: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain2.html
- Domínio 3: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain3.html
- Domínio 4: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/cloud-practitioner-02-domain4.html
- Serviços no escopo: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/clf-02-in-scope-services.html
- Tecnologias e conceitos: https://docs.aws.amazon.com/aws-certification/latest/cloud-practitioner-02/clf-technologies-concepts.html
- Página da certificação: https://aws.amazon.com/certification/certified-cloud-practitioner/
- Seis vantagens da nuvem (Overview of AWS): https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html
- AWS Well-Architected: https://aws.amazon.com/architecture/well-architected/
- AWS CAF: visão geral e jornada: https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/welcome.html
- AWS CAF: capacidades fundamentais: https://docs.aws.amazon.com/whitepapers/latest/overview-aws-cloud-adoption-framework/foundational-capabilities.html
- Estratégias de migração (7 Rs): https://docs.aws.amazon.com/prescriptive-guidance/latest/large-migration-guide/migration-strategies.html
- Modelo de responsabilidade compartilhada: https://aws.amazon.com/compliance/shared-responsibility-model/
- IAM: usuário root e tarefas que exigem root: https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-tasks.html
- IAM: boas práticas de segurança: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
- Segurança, identidade e conformidade: https://aws.amazon.com/products/security/
- Infraestrutura global: Regiões e AZs: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
- Tipos de instância EC2: https://aws.amazon.com/ec2/instance-types/
- Preços do EC2: https://aws.amazon.com/ec2/pricing/
- Classes de armazenamento do S3: https://aws.amazon.com/s3/storage-classes/
- Overview of AWS: Computação: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/compute-services.html

- Overview of AWS: Bancos de dados: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/database.html
- Overview of AWS: Rede: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/networking-services.html
- Overview of AWS: Armazenamento: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/storage-services.html
- Overview of AWS: Gestão e governança: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/management-and-governance.html
- Overview of AWS: Análise de dados: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/analytics.html
- Overview of AWS: Integração de aplicações: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/application-integration.html
- Planos do AWS Support: https://aws.amazon.com/premiumsupport/plans/
- AWS Trusted Advisor: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/
- Preços da AWS: https://aws.amazon.com/pricing/
- Gestão financeira na nuvem: https://aws.amazon.com/aws-cost-management/
- Faturamento consolidado: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html
- Tags de alocação de custos: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html

> **Transparência:** o **AWS Skill Builder** exige login e não foi acessado diretamente; revise o conteúdo por lá. Algumas descrições curtas de serviços (por exemplo, de segurança e de IA/ML) e detalhes como security groups x NACLs foram escritos com base na documentação padrão da AWS, e algumas páginas consultadas traziam pouco detalhe. Números como quantidade de Regiões, desconto máximo e quantidade de verificações do Trusted Advisor mudam com o tempo: confirme nas páginas antes da prova.