Strecht Simulados · Guia de preparação



Guia de preparação SCS-C03

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.

6 capítulos por domínio	**36** questões comentadas	**75%** 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 SCS-C03: 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 75%).

Mapa do exame

Cada prova do curso tem 65 questões e 170 minutos, no formato do exame. Referência de aprovação: 75%.

Domínio (capítulo)	Peso	Neste guia
1. Domínio 1: Detecção	16%	18 conceitos · 13 pegadinhas
2. Domínio 2: Resposta a incidentes	14%	18 conceitos · 14 pegadinhas
3. Domínio 3: Segurança de infraestrutura	18%	18 conceitos · 14 pegadinhas
4. Domínio 4: Gerenciamento de identidade e acesso	20%	18 conceitos · 14 pegadinhas
5. Domínio 5: Proteção de dados	18%	18 conceitos · 14 pegadinhas
6. Domínio 6: Fundamentos de segurança e governança	14%	18 conceitos · 13 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: Detecção

Durante uma investigação de possível exfiltração por túnel DNS, um analista de uma empresa de jogos consulta os VPC Flow Logs de uma instância suspeita e não encontra nenhum registro de tráfego para o servidor DNS da Amazon (o resolvedor da VPC), embora a instância resolva nomes normalmente. Ele precisa ver quais domínios a instância consultou, a partir de agora, com o menor esforço. Qual solução atende a esse requisito?

A. Alterar o formato dos Flow Logs para o formato personalizado com os campos pkt-dstaddr e flow-direction, que passam a registrar o tráfego para o resolvedor
B. Habilitar eventos de dados do Route 53 no CloudTrail da organização para registrar cada consulta DNS feita pelas instâncias da VPC
C. Exportar do GuardDuty os logs de DNS que ele analisa para o S3 da conta de segurança e consultá-los no Athena por instância de origem
D. Configurar o Route 53 Resolver query logging na VPC, enviando os registros para o CloudWatch Logs ou para o S3 com os nomes consultados e o ID da instância

D2 · Domínio 1: Detecção

Uma edtech precisa enviar os logs completos do AWS WAF de um web ACL regional para o SIEM via Amazon Data Firehose. A equipe criou o stream Direct PUT waf-logs-producao na mesma Região do web ACL, mas o stream não aparece como opção ao configurar o logging do web ACL. As permissões do Firehose para o destino já foram testadas com sucesso. Qual ação resolve o problema?

A. Mover o stream do Data Firehose para us-east-1, já que o logging do AWS WAF para o Firehose é centralizado nessa Região
B. Habilitar as requisições amostradas no web ACL e as métricas do CloudWatch nas regras, que são pré-requisito para o logging completo do WAF
C. Adicionar ao bucket de destino do Firehose uma bucket policy para o principal delivery.logs.amazonaws.com com a condição aws:SourceAccount da conta do web ACL
D. Recriar o stream do Data Firehose com nome iniciado por aws-waf-logs-, por exemplo aws-waf-logs-producao, e selecioná-lo na configuração de logging

D3 · Domínio 1: Detecção

Um hospital guarda laudos no prefixo prontuarios/ de um bucket do S3. A auditoria exige saber qual role e qual sessão IAM leu ou apagou cada objeto, receber os registros em poucos minutos e provar que os arquivos de log não foram alterados depois da entrega. O registro de outros prefixos do bucket não é necessário e gera custo. Qual solução atende a esses requisitos?

A. Configurar no trail eventos de dados do S3 com seletor avançado em resources.ARN começando pelo prefixo e ativar a validação de integridade dos arquivos de log
B. Gerar o S3 Inventory diário do prefixo com os campos de última modificação e comparar os relatórios no Athena para identificar a identidade de quem alterou os objetos
C. Manter o trail com eventos de gerenciamento, que já registram GetObject e DeleteObject com o userIdentity da sessão, e ativar a validação de integridade
D. Habilitar os logs de acesso do servidor do S3 com entrega para o CloudWatch Logs e uma política de proteção de dados no log group para preservar os registros

D4 · Domínio 2: Resposta a incidentes

Às 14h05, um ataque de SQL injection alterou saldos de clientes em uma instância do Amazon RDS for PostgreSQL de uma cooperativa de crédito, que tem backups automáticos com retenção de 14 dias. A diretoria quer o banco de volta ao estado das 14h00 o quanto antes, e o jurídico exige preservar a instância comprometida, sem alterações, para análise forense. Qual procedimento atende a esses requisitos?

A. Executar uma restauração para um ponto no tempo às 14h00 em uma instância nova, isolar a instância comprometida por security group e tirar um snapshot dela, e apontar a aplicação para a nova
B. Excluir a instância comprometida gerando um snapshot final para a perícia e restaurar uma instância nova a partir do snapshot automático da madrugada
C. Restaurar o snapshot automático mais recente sobre a instância atual, para manter o mesmo endpoint, e reaplicar os logs de transação até 14h00 pelo console do RDS, mantendo o mesmo grupo de parâmetros
D. Usar o backtrack do RDS para voltar a instância comprometida ao horário das 14h00, preservando o endpoint e evitando a criação de uma instância nova

D5 · Domínio 2: Resposta a incidentes

Uma equipe de segurança identificou, em um exercício de threat hunting, comunicações suspeitas saindo de instâncias EC2 em várias contas de produção de uma organização. Os logs do AWS CloudTrail indicam que uma role do IAM usada entre contas foi provavelmente comprometida e está sendo usada para exfiltrar dados de buckets S3 com informações sensíveis. Os analistas precisam interromper a exfiltração rapidamente, preservar evidências, minimizar o impacto nas aplicações críticas e manter rastreabilidade das ações de resposta. Qual combinação de ações é a MELHOR resposta inicial?

A. Aplicar SCP que nega o uso da role comprometida, isolar as instâncias com security groups de quarentena sem saída, proteger os logs e coletar evidências pela conta de segurança
B. Mover as contas afetadas para uma nova OU com SCP que nega leitura no S3 à role, ativar o AWS Config nas Regiões e reconfigurar à mão as ACLs dos buckets críticos
C. Isolar as instâncias com security group sem saída, ativar o Shield Advanced e o AWS WAF nos endpoints expostos e mover os buckets críticos para uma conta nova
D. Aplicar uma SCP que nega s3:* e sts:AssumeRole nas contas membro, pausar o CloudTrail para reduzir ruído e encerrar as instâncias suspeitas guardando só snapshots

D6 · Domínio 2: Resposta a incidentes

Um finding do GuardDuty mostra que uma instância EC2 da conta Loja se comunicou com o IP 198.51.100.77, associado a uma campanha de malware. A organização tem o Amazon Detective habilitado com administrador delegado na conta Security, e todas as contas membro fazem parte do behavior graph. Antes de conter, o líder do incidente quer saber rapidamente quais outros recursos de qualquer conta trocaram tráfego com esse IP e se ele fez chamadas de API, sem escrever consultas. Qual ação atende ao requisito?

A. Abrir no Amazon Detective o perfil da entidade do endereço IP 198.51.100.77 e analisar os painéis de interação com recursos e de chamadas de API no período do incidente
B. Executar uma análise do Network Access Analyzer em cada VPC para identificar os recursos com caminho de rede alcançável a partir do endereço 198.51.100.77
C. Executar consultas no Amazon Athena sobre os VPC Flow Logs e o trail da organização para encontrar conexões e chamadas de API envolvendo o endereço 198.51.100.77
D. Filtrar no console do GuardDuty da conta Security os findings cujo remoteIpDetails seja igual a 198.51.100.77, para listar os recursos de cada conta afetada

D7 · Domínio 3: Segurança de infraestrutura

Uma empresa de e-commerce usa uma VPC com sub-redes públicas e privadas em várias zonas de disponibilidade. A equipe de segurança precisa garantir que só instâncias EC2 específicas, em uma sub-rede privada, acessem um cluster Amazon RDS também privado. O acesso administrativo às instâncias deve passar por um bastion host na sub-rede pública, sem abrir SSH/RDP para a internet. Qual combinação atende a esses requisitos com o menor aumento de superfície de ataque?

A. SG do RDS aceitando o SG das instâncias autorizadas; SG do bastion com SSH/RDP do IP fixo da equipe; esse mesmo SG do bastion anexado às instâncias privadas
B. SG do RDS aceitando a sub-rede privada inteira; NACL liberando SSH/RDP da internet para a sub-rede privada e bloqueando as demais portas
C. SG do RDS aceitando o SG das instâncias autorizadas; SG do bastion com SSH/RDP do IP fixo da equipe; instâncias privadas aceitando SSH/RDP do SG do bastion
D. SG do RDS aceitando a VPC inteira; NACL liberando a saída das instâncias para o RDS; bastion com SSH/RDP aberto para a internet e acesso controlado por IAM

D8 · Domínio 3: Segurança de infraestrutura

Um banco conecta o data center à AWS por uma conexão dedicada de 10 Gbps do AWS Direct Connect. A auditoria interna passou a exigir criptografia do enlace entre o roteador do banco e o dispositivo da AWS no local do Direct Connect, na camada 2, sem reduzir a vazão da conexão e sem depender de cada aplicação implementar criptografia. O roteador de borda do banco suporta MACsec. Qual solução atende a esses requisitos?

A. Criar uma AWS Site-to-Site VPN sobre uma interface virtual pública do Direct Connect e rotear o tráfego do data center pelos túneis IPsec
B. Contratar uma conexão hospedada de um parceiro do Direct Connect com MACsec, associar a chave CKN/CAK à conexão hospedada e migrar as interfaces virtuais
C. Exigir TLS 1.2 ou superior nos serviços expostos pela VPC e bloquear nos security groups as portas de protocolos sem criptografia
D. Habilitar MACsec na conexão dedicada, associar um par CKN/CAK com associate-mac-sec-key, configurar o mesmo par no roteador e usar o modo must_encrypt

D9 · Domínio 3: Segurança de infraestrutura

Uma empresa usa o Session Manager do AWS Systems Manager para administrar instâncias Amazon EC2 em sub-redes privadas, sem IP público e sem rota para a internet. O time de segurança quer que todo o tráfego do SSM Agent e das sessões permaneça na rede da AWS. Qual configuração atende a esse requisito com o menor esforço operacional?

A. Endpoint de interface só para com.amazonaws.região.ssm, sem o endpoint de ssmmessages
B. Endpoints de interface para ssm, ssmmessages e ec2messages, com HTTPS liberado no security group
C. NAT gateway em uma sub-rede pública, com rota para a internet a partir das sub-redes privadas
D. Gateway endpoint do S3 nas tabelas de rota privadas, transportando o tráfego do SSM Agent e das sessões

D10 · Domínio 4: Gerenciamento de identidade e acesso

Em uma seguradora, a role dos administradores de banco de dados usa uma chave KMS gerenciada pelo cliente para criar e operar instâncias RDS criptografadas em sa-east-1. A segurança descobriu que essa role também chama kms:Decrypt diretamente pelo CLI para descriptografar arquivos que outra equipe cifrou com a mesma chave. A exigência é que os DBAs só consigam usar a chave por meio do RDS nessa Região, sem afetar outros serviços que usam a chave. Qual statement da key policy, substituindo a permissão atual da role, atende a esse requisito?

A. Permitir à role dos DBAs as ações de criptografia da chave com a condição aws:CalledVia igual a rds.amazonaws.com
B. Permitir à role dos DBAs as ações de criptografia da chave com a condição kms:CallerAccount igual ao ID da conta dos bancos
C. Permitir à role dos DBAs as ações de criptografia da chave com a condição kms:ViaService igual a rds.sa-east-1.amazonaws.com
D. Permitir à role dos DBAs as ações de criptografia da chave com a condição aws:SourceVpce igual ao endpoint do RDS na VPC

D11 · Domínio 4: Gerenciamento de identidade e acesso

Para padronizar, uma equipe de uma empresa de educação passou a criar as roles de execução das funções Lambda a partir de um template copiado das roles de instâncias EC2, apenas trocando as políticas de permissão. Ao criar uma função com uma dessas roles, o deploy falha com InvalidParameterValueException: The role defined for the function cannot be assumed by Lambda. O usuário do pipeline tem iam:PassRole para a role. Qual correção resolve o erro com o menor privilégio?

A. Trocar o Principal da trust policy da role de ec2.amazonaws.com para lambda.amazonaws.com com a ação sts:AssumeRole
B. Anexar à role a política gerenciada AWSLambdaBasicExecutionRole, que concede ao serviço Lambda a permissão de assumir a role de execução
C. Adicionar à função uma resource-based policy que permita lambda:InvokeFunction ao service principal lambda.amazonaws.com na conta
D. Conceder ao usuário do pipeline sts:AssumeRole na role de execução, para que ele assuma a role em nome do Lambda durante o deploy

D12 · Domínio 4: Gerenciamento de identidade e acesso

A equipe de plataforma de uma fabricante de veículos publica pacotes de agentes de segurança em um bucket do S3 na conta de ferramentas. As 230 contas da organização, de todas as OUs, precisam baixar esses pacotes, e contas entram e saem da organização toda semana. A bucket policy atual lista os IDs de conta um a um e vive desatualizada. A segurança quer permitir a leitura a qualquer principal das contas da organização e a nenhum outro, sem manutenção da lista. Qual instrução na bucket policy atende a esse requisito?

A. Allow em s3:GetObject para o Principal "*" com a condição StringEquals aws:PrincipalOrgID igual ao ID da organização no recurso do bucket de pacotes
B. Allow em s3:GetObject para o Principal "*" com a condição StringEquals aws:SourceOrgID igual ao ID da organização no recurso do bucket de pacotes
C. Allow em s3:GetObject para o Principal da conta de gerenciamento da organização, com a expectativa de que o acesso seja herdado pelas contas membro da organização
D. Allow em s3:GetObject para o Principal "*" com a condição ForAnyValue:StringLike aws:PrincipalOrgPaths igual ao caminho da OU de produção da organização

01

CAPÍTULO 1 · 16% DA PROVA

Domínio 1: Detecção

Aqui eu preciso saber qual fonte de log responde a cada pergunta (CloudTrail, VPC Flow Logs, Resolver query logs, server access logs, logs do ALB e do WAF) e qual serviço detecta, agrega ou alerta (GuardDuty, Security Hub CSPM, Macie, Inspector, Config, Security Lake, EventBridge). A prova descreve um sintoma bem específico, como 'o finding aparece no console mas o alerta não chega' ou 'faltam eventos de uma Região', e pede a causa ou a solução com menor esforço. Quase sempre há uma alternativa que usa o log errado para a pergunta (Flow Logs para nome de domínio, CloudTrail de gerenciamento para download de objeto). Onde mais erro: esquecer que muita coisa é regional (regras do EventBridge, administrador delegado, threat lists do GuardDuty) e confundir supressão de falso positivo com redução de alerta.

Neste capítulo

18 tópicos-chave · 13 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Eventos de gerenciamento x eventos de dados do CloudTrail

GetObject e outras leituras de objeto são eventos de dados e não aparecem em um trail só com eventos de gerenciamento; PutBucketPolicy é evento de gerenciamento. Para auditar downloads de um bucket sem explodir custo, use advanced event selectors filtrando resources.ARN e eventName. O histórico de eventos é por conta e Região, só de gerenciamento, sem prova de integridade.

Validação de integridade do CloudTrail

Gera arquivos digest a cada hora, com hash SHA-256 e assinatura RSA, provando que os logs não foram alterados nem apagados. Combine com trail da organização, conta de log dedicada e Object Lock para auditoria imutável. Nunca pare o trail para 'preservar' evidência.

Trail da organização e multi-Região

Logs centrais que as contas membro não alteram vêm de um trail da organização gravando em conta de log dedicada. Trail criado pela CLI nasce de uma Região só: se faltam eventos de uma Região, confira IsMultiRegionTrail. Erro InsufficientS3BucketPolicyException pede ajuste da bucket policy para o principal de serviço cloudtrail.amazonaws.com.

VPC Flow Logs

Mostram quem falou com quem, porta, bytes e ação de aceite ou rejeição, mas não registram chamadas de API, nomes de domínio, tráfego para o DNS da Amazon nem para o IMDS. Atrás de NAT gateway ou transit gateway, acrescente pkt-srcaddr e pkt-dstaddr ao formato personalizado. No S3, Parquet, partições compatíveis com Hive e partição horária reduzem o custo do Athena.

Route 53 Resolver query logs

É a fonte para saber qual domínio uma instância consultou. Query logging de hosted zone pública só vê consultas autoritativas, e o CloudTrail não registra resolução de nomes.

GuardDuty com administrador delegado

Detecção gerenciada de ameaças em várias contas: administrador delegado com auto-enable, designado em cada Região usada. Threat lists (feed próprio) e suppression rules são criadas no administrador; trusted list faz o contrário de threat list, silencia. Proteções adicionais: S3 Protection (acesso anômalo a objetos, sem configurar data events no trail), RDS Protection (login anômalo em Aurora e RDS, sem agente), Runtime Monitoring (processo, shell, mineração dentro do contêiner) e EKS Audit Log Monitoring (chamadas à API do cluster).

GuardDuty Extended Threat Detection

Correlaciona estágios de um ataque em um único achado crítico do tipo AttackSequence, sem regra própria. Achados arquivados por supressão não entram nas sequências, por isso o filtro de supressão deve ser estreito (tipo do finding + AMI ou tag).

GuardDuty Malware Protection for S3

Varre arquivos enviados ao bucket e marca o objeto com tag do resultado; uma bucket policy pela tag impede o uso antes da varredura. S3 Protection, ao contrário, analisa eventos de acesso e não inspeciona o conteúdo dos arquivos.

Security Hub CSPM x exposure findings do Security Hub

Security Hub CSPM avalia controles e padrões (PCI DSS, CIS, FSBP) e agrega achados de várias contas e Regiões; a maior parte dos controles depende de regras do AWS Config gravando os tipos de recurso (controle com WARNING e Config.1 FAILED = Config não está gravando). Exposure findings priorizam a combinação de vulnerabilidade, exposição e permissão com caminho de ataque.

Custom action x evento Imported do Security Hub

Custom action envia ao EventBridge só o achado que o analista escolheu no console. O evento Imported dispara para todos os achados, sempre. Insights apenas agrupam e filtram no console, não enviam nada.

Amazon Macie

Descobre e classifica dados sensíveis no S3. Descoberta automatizada dá visão ampla e contínua com custo controlado; job faz análise completa de um alvo. Formatos proprietários (matrícula, ID de funcionário) pedem custom data identifier com regex, keywords e proximidade; allow list serve para ignorar padrões.

Amazon Security Lake

Centraliza logs em OCSF e Parquet; fonte de terceiros entra como fonte personalizada nesse formato. Assinante com acesso de consulta (Lake Formation) consulta sem copiar; assinante com acesso a dados ingere. WAF é fonte nativa.

CloudWatch: Logs Insights, filtro de métrica e detecção de anomalias

Pergunta pontual sobre logs que já estão no CloudWatch: Logs Insights. Métrica contínua daqui para frente: filtro de métrica com alarme e SNS. Métrica sazonal com alarme estático ruidoso: alarme de detecção de anomalias, sem modelo para manter. Pico anormal de chamadas de API ou de erros: CloudTrail Insights.

Arquivamento de CloudWatch Logs

Para guardar por anos: retenção curta no log group + subscription filter para Firehose gravar no S3 + Lifecycle. Export task é pontual, pode levar até 12 horas para disponibilizar os dados e não serve como arquivamento contínuo.

Logs de acesso de borda e de API

Caminho, user agent e status HTTP estão nos logs de acesso do ALB e do CloudFront. No API Gateway, quem chamou, de qual IP e com qual status vem do access logging com $context.identity.sourceIp; execution logs são para depurar. Sem logs no API Gateway com erro de role ARN: falta o cloudWatchRoleArn nas configurações da conta, por Região.

AWS Config: regras, conformance packs e State Manager

Mudança de configuração que deixou algo público: regra gerenciada do Config + EventBridge (Compliance Change) + SNS. Regras e remediações em pacote para várias contas: conformance packs. Garantir de forma contínua que um agente esteja instalado: associação do State Manager; execução única é Run Command.

Alertas multi-conta com EventBridge

Regras do EventBridge são regionais: o finding visível no console sem alerta indica falta de regra na mesma Região do finding. Para várias contas, regras em cada conta e Região (via StackSets) encaminham ao barramento central. Filtro por severidade do GuardDuty usa correspondência numérica em detail.severity.

Logs que não aparecem

WAF exige prefixo aws-waf-logs- no nome do destino. Network Firewall precisa de logging configuration (ALERT e FLOW). Lambda sem log: faltam logs:CreateLogGroup, CreateLogStream e PutLogEvents na execution role. Agente do CloudWatch com AccessDenied: falta CloudWatchAgentServerPolicy na role da instância. Log legado do CloudFront em bucket novo falha com ACLs desabilitadas.

Macetes para memorizar

💡 Fonte de log certa

DNS = Resolver. Rede = Flow Logs. API = CloudTrail. HTTP = logs do ALB/CloudFront.

💡 Pipeline de achados

GuardDuty detecta, Security Hub CSPM agrega, EventBridge distribui, Firehose arquiva.

💡 Regionalidade

Administrador delegado, regra do EventBridge e threat list: uma por Região, sempre.

💡 Threat x trusted list

Threat list grita, trusted list cala.

💡 Pergunta x vigilância

Pergunta de agora = Logs Insights; vigiar daqui pra frente = filtro de métrica.

💡 Macie

Automatizada é radar amplo; job é lupa num alvo.

Tabela de memorização: não confunda

Quando é...	...e quando é
VPC Flow Logs Quem falou com quem, porta, bytes, aceito ou rejeitado.	**Route 53 Resolver query logs** Qual nome de domínio a instância consultou; Flow Logs nem enxergam o tráfego para o DNS da Amazon.
Eventos de dados do CloudTrail Identidade IAM de quem leu ou apagou o objeto, integridade validável e filtro por prefixo.	**Server access logs do S3** Falha de autenticação, operações de lifecycle e prova de downloads passados quando não havia eventos de dados habilitados; entrega em melhor esforço.
Suppression rule do GuardDuty Falso positivo conhecido (scanner autorizado), com filtro estreito por tipo + AMI ou tag.	**Filtro numérico de severidade no EventBridge** Reduzir o volume de alertas enviados ao plantão sem esconder achados dos analistas.

CloudWatch Logs Insights Pergunta pontual sobre logs já existentes (ex.: contagem por IP nas últimas horas).	**Filtro de métrica + alarme** Monitoramento contínuo daqui para frente de uma chamada de API ou padrão de log.
Descoberta automatizada do Macie Visão ampla e contínua de dados sensíveis com custo controlado.	**Job do Macie** Análise completa de um bucket ou alvo específico.
GuardDuty Runtime Monitoring Ameaça dentro do contêiner: processo, shell, mineração.	**EKS Audit Log Monitoring** Chamadas suspeitas à API do cluster Kubernetes.
Cost Anomaly Detection Gasto fora do padrão sem limite fixo definido.	**Budgets ou alarme de faturamento** Limite de custo definido por você.

Números que caem

Item	Valor
Digest de integridade do CloudTrail	**a cada hora, SHA-256 + RSA**
Disponibilização de dados de uma export task do CloudWatch Logs	**pode levar até 12 horas**
Severidade alta ou crítica do GuardDuty no EventBridge	**detail.severity numérico maior ou igual a 7**
Região das métricas de health check do Route 53	**us-east-1**
Prefixo obrigatório do destino de logs do WAF	**aws-waf-logs-**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar VPC Flow Logs para descobrir qual domínio malicioso a instância resolveu.
Como não cair: Flow Logs não mostram nomes nem capturam tráfego para o servidor DNS da Amazon; a fonte é Resolver query logs.

⚠ **Alerta de prova:** Achar que um trail só com eventos de gerenciamento registra quem baixou objetos do S3.
Como não cair: GetObject é evento de dados; sem data events habilitados, o download não aparece no trail.

⚠ **Alerta de prova:** Criar suppression rule ampla para diminuir o barulho de alertas do plantão.
Como não cair: Supressão arquiva o achado e o tira da fila dos analistas e das sequências do Extended Threat Detection; para reduzir alerta, filtre severidade na regra do EventBridge.

⚠ **Alerta de prova:** Criar a suppression rule ou a threat list na conta membro.
Como não cair: Em ambiente multi-conta só o administrador do GuardDuty cria regras de supressão e listas, e em cada Região.

⚠ **Alerta de prova:** Propor CloudTrail Lake como repositório de consulta para uma conta nova.
Como não cair: CloudTrail Lake está fechado a novos clientes; consulte o trail no S3 com Athena (com partition projection para não manter partições).

⚠ **Alerta de prova:** Usar export task periódica do CloudWatch Logs como arquivamento contínuo.
Como não cair: Export task é pontual, pode levar até 12 horas e falhas deixam lacunas; use subscription filter para Firehose e S3.

⚠ **Alerta de prova:** Recorrer ao AWS Config para alertar sobre uma chamada de API específica ou comportamento anômalo de credencial.
Como não cair: Config avalia estado de configuração; chamada de API específica é CloudTrail + EventBridge ou filtro de métrica, e uso malicioso de credencial é GuardDuty.

⚠ **Alerta de prova:** Usar Inspector para monitorar logins em RDS ou Malware Protection para achar CVEs.
Como não cair: Inspector avalia vulnerabilidades em EC2, imagens e Lambda; login anômalo em banco é GuardDuty RDS Protection; malware não é CVE.

⚠ **Alerta de prova:** Configurar a regra do EventBridge em uma Região central esperando receber findings de outra Região.
Como não cair: A regra precisa existir na Região do finding e de lá encaminhar ao barramento ou tópico central.

⚠ **Alerta de prova:** Criar um VPC endpoint para resolver uma Lambda que não grava logs.
Como não cair: Os logs são enviados pelo serviço Lambda; o problema é permissão de logs na execution role.

⚠ **Alerta de prova:** Usar Traffic Mirroring para descobrir o IP real atrás de NAT gateway.
Como não cair: Basta acrescentar pkt-srcaddr e pkt-dstaddr ao formato do flow log; mirroring custa e opera muito mais.

⚠ **Alerta de prova:** Mudar o caminho para Flow Logs no CloudWatch Logs para baratear consultas.
Como não cair: O próprio destino S3 oferece Parquet e partição horária; levar para o CloudWatch aumenta custo de ingestão.

⚠ **Alerta de prova:** Resolver bucket policy de log com permissão de KMS na key policy.
Como não cair: A key policy só importa quando o bucket usa SSE-KMS com chave do cliente; com SSE-S3 o erro é de ACL ou bucket policy.

Como cai na prova

📝 **Como cai:** Sintoma de log ausente: 'o finding aparece mas não chega alerta' ou 'faltam eventos de uma Região'.
Como resolver: Procure o detalhe regional ou de configuração: regra do EventBridge na Região do finding, IsMultiRegionTrail, prefixo aws-waf-logs-, permissão de logs na role. Descarte alternativas que trocam de serviço.

📝 **Como cai:** Pergunta investigativa: quem fez, de onde, qual objeto ou qual domínio.
Como resolver: Mapeie a pergunta para a fonte: identidade e API = CloudTrail (dados se for objeto), domínio = Resolver query logs, conexão = Flow Logs, HTTP = logs de acesso.

📝 **Como cai:** Detecção em várias contas 'com o menor esforço operacional' e incluindo contas futuras.
Como resolver: Serviço gerenciado com administrador delegado e auto-enable, ou StackSets com implantação automática na organização. Descarte Lambda agendada, scripts e configuração conta por conta.

📝 **Como cai:** Excesso de alertas ou falso positivo de scanner autorizado.
Como resolver: Falso positivo conhecido: suppression rule estreita no administrador. Volume de alerta: filtro de severidade no EventBridge. Nunca esconder achados de toda a frota.

📝 **Como cai:** Centralizar e consultar logs de segurança para SIEM.
Como resolver: Security Lake em OCSF; assinante de consulta se o SIEM consulta sem copiar, de dados se precisa ingerir; fonte de terceiros como fonte personalizada.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
qual domínio a instância consultou	**Route 53 Resolver query logs**
ataque em vários estágios virando um único achado crítico	**GuardDuty Extended Threat Detection (AttackSequence)**
arquivo enviado por usuário precisa ser varrido antes do uso	**GuardDuty Malware Protection for S3 + bucket policy pela tag do resultado**

exfiltração anômala no S3 sem código e sem data events	**GuardDuty S3 Protection**
InstanceCredentialExfiltration.OutsideAWS	**Credencial do instance profile usada fora da AWS: revogar sessões da role e exigir IMDSv2**
pico anormal de chamadas de API ou de erros, sem limite definido	**CloudTrail Insights**
analista escolhe o achado no console e envia ao ticket	**Custom action do Security Hub CSPM + EventBridge**
formato proprietário de identificador sensível	**Custom data identifier do Macie (regex + keywords + proximidade)**
instância sem SSM Agent no Inspector	**Modo de varredura híbrido (sem agente, via snapshot do EBS)**
visibilidade de tráfego entre VPCs num hub de transit gateway	**Transit gateway flow logs**
alarme de health check do Route 53 não aparece	**Métricas do Route 53 só existem em us-east-1**
logs de várias contas em tempo real para um Kinesis central	**Destino do CloudWatch Logs + subscription filters, policy com aws:PrincipalOrgID**
painel Grafana multi-conta sem servidor	**Amazon Managed Grafana em administrador delegado, não na conta de gerenciamento**
central de notificações com e-mail e chat, sem Lambda	**AWS User Notifications**

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

- GetObject é evento de dados: trail só de gerenciamento não registra download.
- Flow Logs não mostram DNS da Amazon nem IMDS, e nunca mostram nomes de domínio.
- Supressão arquiva o achado: use só para falso positivo conhecido, com filtro estreito, no administrador.
- Regras do EventBridge e administradores delegados são regionais.
- Security Hub CSPM depende do AWS Config gravando os recursos.

Essenciais para a prova (checklist)

- ☐ Sei escolher entre CloudTrail, Flow Logs, Resolver query logs, server access logs e logs do ALB para cada pergunta investigativa.
- ☐ Sei habilitar eventos de dados do S3 com advanced event selectors para um bucket específico.
- ☐ Sei montar auditoria imutável com trail da organização, validação de integridade e Object Lock.
- ☐ Sei diferenciar suppression rule, trusted list, threat list e filtro de severidade no EventBridge.

- ☐ Sei qual proteção do GuardDuty cobre S3, RDS, contêiner em execução, API do EKS e malware em uploads.
- ☐ Sei arquivar CloudWatch Logs por anos com subscription filter, Firehose e Lifecycle.
- ☐ Sei diagnosticar log ausente de WAF, Network Firewall, Lambda, API Gateway e agente do CloudWatch.
- ☐ Sei configurar Security Lake com fonte personalizada e assinantes de consulta ou de dados.
- ☐ Sei quando usar Logs Insights, filtro de métrica, detecção de anomalias e CloudTrail Insights.

Questões de revisão do capítulo

R1.1 · Domínio 1: Detecção

Um banco digital centraliza a telemetria de segurança no Amazon Security Lake e quer incluir os logs de um firewall de nova geração de terceiros que roda nos data centers. A equipe já tem um coletor que recebe os eventos por syslog e pode transformá-los. Os analistas querem consultar esses eventos no Athena junto com VPC Flow Logs e CloudTrail, no mesmo esquema, e os assinantes atuais do data lake devem passar a recebê-los sem integração extra. Qual solução atende a esses requisitos?

A. Adicionar uma fonte personalizada no Security Lake e fazer o coletor gravar os eventos em OCSF e Parquet no prefixo atribuído, usando a role criada
B. Gravar os eventos brutos em JSON no bucket do Security Lake em um prefixo próprio e criar uma tabela própria no Athena apontando para esse prefixo
C. Enviar os eventos do coletor ao CloudWatch Logs em um grupo dedicado e habilitar esse grupo como fonte nativa do Security Lake em cada Região
D. Cadastrar o fornecedor do firewall como assinante com acesso a dados no Security Lake para que ele publique os eventos no data lake da empresa

R1.2 · Domínio 1: Detecção

Uma rede de varejo usa o Amazon GuardDuty com administrador delegado na conta Security e uma regra do Amazon EventBridge que envia todo finding a um tópico do Amazon SNS assinado pelo plantão. O plantão recebe centenas de e-mails por dia e passou a ignorá-los. A equipe quer que o SNS receba só findings de severidade alta ou crítica (7.0 ou mais), sem deixar de registrar no GuardDuty os demais findings para análise posterior. Qual alteração atende ao requisito?

A. Criar no GuardDuty um filtro de supressão para findings com severidade menor que 7, para que só os findings altos e críticos sigam para o EventBridge e para o SNS
B. Alterar a frequência de exportação de findings atualizados do GuardDuty de 15 minutos para 6 horas, para reduzir o volume de notificações recebidas pelo plantão
C. Alterar o padrão de evento da regra para source aws.guardduty e detail.severity igual à string HIGH ou CRITICAL, mantendo o tópico do SNS como destino da regra
D. Alterar o padrão de evento da regra para source aws.guardduty, detail-type GuardDuty Finding e detail.severity com correspondência numérica maior ou igual a 7.0

R1.3 · Domínio 1: Detecção

Uma universidade usa o Amazon Macie para encontrar dados pessoais em seus buckets S3, mas os números de matrícula dos alunos, no formato MAT seguido de hífen e 8 dígitos, não aparecem em nenhum achado. Os arquivos do almoxarifado também usam códigos de material com o mesmo padrão, e esses não devem gerar achados. A equipe sabe que as matrículas costumam aparecer perto das palavras matrícula ou aluno. Qual solução atende a esses requisitos?

A. Criar um identificador de dados personalizado com a regex MAT-[0-9]{8}, as palavras-chave matrícula e aluno e uma distância máxima, usando-o nos jobs e na descoberta automatizada
B. Criar uma regra do EventBridge que filtre os achados do Macie com a regex MAT-[0-9]{8} e encaminhe para o time de privacidade os que contiverem matrícula ou aluno no trecho de amostra do achado
C. Habilitar o identificador de dados gerenciado de número de identificação nacional, que reconhece formatos de documento de identificação de estudantes no Brasil
D. Criar uma allow list com a regex MAT-[0-9]{8} e as palavras matrícula e aluno, para que o Macie passe a reportar as ocorrências desse padrão nos buckets

R1.4 · Domínio 1: Detecção

Uma equipe de segurança precisa detectar automaticamente atividades suspeitas em uma conta AWS recém-criada, incluindo uso de chaves de acesso expostas publicamente, tentativas de acesso a partir de países incomuns e escalonamento de privilégios. A conta faz parte de uma organização AWS Organizations com múltiplas contas. A equipe deseja uma solução gerenciada que centralize os achados de segurança em uma conta de segurança dedicada, permitindo automação de resposta por meio de AWS Security Hub e AWS Lambda. Qual abordagem atende melhor a esses requisitos com o menor esforço operacional?

A. Criar regras personalizadas do AWS Config em cada conta para detectar padrões de uso suspeito de IAM e configurar um aggregator do AWS Config para centralizar os resultados em uma única conta.
B. Ativar o Amazon GuardDuty nas contas e Regiões, definir a conta de segurança como administradora delegada do GuardDuty na organização e integrar os achados ao AWS Security Hub para automação.
C. Configurar o CloudWatch Logs Insights em cada conta para consultar VPC Flow Logs e eventos do CloudTrail sob demanda quando houver suspeita de incidente e acionar execuções do Systems Manager Automation.
D. Ativar o AWS CloudTrail em cada conta, enviar os logs para um bucket S3 central e configurar consultas recorrentes no Amazon Athena para identificar atividades suspeitas, disparando notificações via Amazon SNS.

Respostas comentadas

R1.1. A) Adicionar uma fonte personalizada no Security Lake e fazer o coletor gravar os eventos em OCSF e Parquet no prefixo atribuído, usando a role criada

Por quê: O Amazon Security Lake normaliza dados em OCSF e Parquet. Fontes de terceiros entram como fontes personalizadas: o produtor converte para OCSF (uma classe de evento por fonte, como Network Activity para firewall), segue o particionamento region/accountId/eventDay e grava no prefixo da fonte usando a role criada pelo Security Lake. Assinantes de dados ou de consulta recebem tudo pelo mesmo esquema.

✗ B) Incorreta. Dados fora de OCSF e Parquet e fora da estrutura de fonte personalizada não entram no catálogo e nas tabelas do Lake Formation do Security Lake, ficando fora do esquema comum e dos assinantes.

✗ C) Incorreta. CloudWatch Logs não é uma fonte nativa do Security Lake; as fontes nativas incluem CloudTrail, VPC Flow Logs, Route 53 Resolver query logs, achados do Security Hub, logs de auditoria do EKS e logs do AWS WAF.

✗ D) Incorreta. Assinantes consomem dados do data lake; quem envia dados é uma fonte, nativa ou personalizada.

> **Dica de prova:** Log de terceiro no Security Lake: fonte personalizada em OCSF e Parquet. Quem lê: assinante.

R1.2. D) Alterar o padrão de evento da regra para source aws.guardduty, detail-type GuardDuty Finding e detail.severity com correspondência numérica maior ou igual a 7.0

Por quê: O GuardDuty publica cada finding no EventBridge com a severidade como número no campo detail.severity. Padrões de evento do EventBridge aceitam correspondência numérica, o que permite rotear só faixas de severidade a um destino sem suprimir nada no GuardDuty. Findings arquivados por supressão não são enviados ao EventBridge.

✗ A) Incorreta. Regras de supressão arquivam automaticamente os findings e eles deixam de ir ao EventBridge, mas também saem da fila de trabalho dos analistas, o que esconde achados que deveriam ser analisados.

✗ B) Incorreta. A frequência só agrupa as ocorrências seguintes de findings já existentes; cada finding novo continua gerando um evento quase em tempo real, seja qual for a severidade.

✗ C) Incorreta. O campo severity do finding é numérico; um padrão com strings como HIGH não corresponde a nenhum evento e o plantão deixaria de receber até os findings críticos.

> **Dica de prova:** Filtrar findings do GuardDuty por severidade: padrão do EventBridge com numeric em detail.severity; supressão serve para falso positivo conhecido, não para reduzir alerta.

R1.3. A) Criar um identificador de dados personalizado com a regex MAT-[0-9]{8}, as palavras-chave matrícula e aluno e uma distância máxima, usando-o nos jobs e na descoberta automatizada

Por quê: Identificadores de dados personalizados do Macie são compostos por uma regex obrigatória e, opcionalmente, palavras-chave, palavras a ignorar e uma regra de proximidade (distância máxima entre a palavra-chave e o texto encontrado). Eles complementam os identificadores gerenciados em jobs e na descoberta automatizada e podem ter severidade própria por número de ocorrências.

✗ B) Incorreta. Se nenhum identificador detecta o padrão, o Macie não gera achados para filtrar; a regra não teria o que encaminhar.

✗ C) Incorreta. Identificadores gerenciados reconhecem formatos públicos padronizados; um código interno da universidade não corresponde a nenhum deles.

✗ D) Incorreta. Allow lists fazem o contrário: definem texto que o Macie deve ignorar; elas não criam novos critérios de detecção.

> **Dica de prova:** Formato proprietário (matrícula, ID de funcionário): custom data identifier com regex + keywords + proximidade. Allow list é para ignorar.

R1.4. B) Ativar o Amazon GuardDuty nas contas e Regiões, definir a conta de segurança como administradora delegada do GuardDuty na organização e integrar os achados ao AWS Security Hub para automação.

Por quê: O Amazon GuardDuty analisa eventos do CloudTrail, VPC Flow Logs e logs de DNS com inteligência de ameaças e aprendizado de máquina, gerando achados como UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration e PrivilegeEscalation:IAMUser/AnomalousBehavior. Com uma conta de segurança como administradora delegada na organização, as contas membro, inclusive as novas, são habilitadas automaticamente, e os achados seguem para o Security Hub e o EventBridge para resposta automatizada.

✗ A) Incorreta. O AWS Config avalia configuração de recursos, não comportamento anômalo de credenciais, e regras personalizadas exigem desenvolvimento.

✗ C) Incorreta. Consultas sob demanda dependem de alguém suspeitar do incidente; não há detecção contínua nem centralização dos achados.

✗ D) Incorreta. Exige escrever e manter consultas próprias e não traz a inteligência de ameaças de um serviço gerenciado de detecção.

> **Dica de prova:** Detecção gerenciada de ameaças em várias contas: GuardDuty com administrador delegado e auto-enable.

02

CAPÍTULO 2 · 14% DA PROVA

Domínio 2: Resposta a incidentes

Neste domínio eu preciso saber conter, coletar evidência, investigar e recuperar sem destruir prova: a ordem dos passos é cobrada tanto quanto o serviço. A prova traz uma EC2, pod, Lambda, credencial ou chave KMS comprometida e oferece alternativas que encerram, apagam ou alteram o recurso antes da coleta. Também cai muito a contenção que não funciona: trocar trust policy ou instance profile não derruba sessões já emitidas, e trocar security group não corta conexão rastreada. Onde mais erro: esquecer o Auto Scaling group levando a instância, confundir Detective (investigação) com GuardDuty (detecção) e escolher ação irreversível (agendar exclusão de chave, apagar segredo) quando havia uma reversível.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 6 macetes · 13 gatilhos · 4 questões comentadas

Tópicos-chave

Ordem forense em EC2

Primeiro capture os metadados (DescribeInstances, ENIs, associação do instance profile) e grave no bucket forense com Object Lock, porque a contenção muda security groups, role e tags. Isolar com security group de quarentena não apaga memória nem disco; capture a memória (Run Command) antes do snapshot do EBS, analise em ambiente isolado e restaure de AMI confiável. Nunca encerrar nem parar antes de coletar: a memória volátil se perde. AMI da instância comprometida leva o comprometimento adiante.

Instância em Auto Scaling group

Primeiro desanexe a instância ou coloque em Standby, depois isole; senão o ASG a substitui por health check e leva a evidência. Termination protection do EC2 e proteção contra scale-in não impedem a substituição de instância não saudável.

Contenção de credencial temporária roubada

Sessões já emitidas valem até expirar mesmo se a trust policy ou o instance profile mudarem. Use Revoke active sessions (AWSRevokeOlderSessions), que nega por aws:TokenIssueTime. Para achar o escopo, pivote pelo accessKeyId (ASIA...) no trail, não pelo nome da role.

Credencial de usuário IAM suspeita

Conter (chaves Inactive + Deny explícito), investigar no CloudTrail e rotacionar; excluir só depois da investigação. Remover políticas apaga o estado de permissões que a análise precisa.

Rastreamento de conexão do security group

Trocar o security group não derruba conexões já rastreadas; a sessão do atacante continua. Corte imediato: regra Deny na NACL, que é stateless.

Contenção reversível de chave KMS

DisableKey/EnableKey, liberados na key policy para a role de resposta, bloqueiam e reativam na hora. Exclusão agendada é irreversível depois do prazo. DeleteImportedKeyMaterial só vale para chave com material importado (origem EXTERNAL). Uso indevido de chave por um usuário: conter o principal, porque a chave em si não vazou.

Segredo vazado ou excluído

Segredo vazado: rotacionar, não apagar; quem leu aparece no CloudTrail filtrando GetSecretValue pelo ARN do segredo. Segredo excluído: RestoreSecret dentro da janela de recuperação (7 a 30 dias, padrão 30); só ForceDeleteWithoutRecovery apaga sem volta.

Incidente em Lambda

Coletar código, configuração e logs imutáveis antes de corrigir. Para parar a função sem destruir evidência: concorrência reservada 0. Apagar função e role elimina evidência.

Forense em EKS

Pod comprometido: network policy deny-all, cordon do nó, proteção contra término, captura de memória e depois snapshot. Excluir o pod ou fazer drain e encerrar o nó destrói a evidência em execução.

Amazon Detective

Investiga escopo e causa raiz de um achado do GuardDuty com histórico do principal e perfil de entidade de IP ('quem mais falou com este IP?'). Só enxerga dados a partir de quando foi habilitado; não executa SQL próprio. Para linha do tempo com logs já no S3, use Athena sobre CloudTrail e Flow Logs.

AWS Config timeline x CloudTrail

O que mudou e como era antes: AWS Config (timeline). Quem chamou a API: CloudTrail. A timeline do Config junta os dois; Flow Logs não mostram quem alterou um security group.

Resposta automatizada e auditável

EventBridge + runbooks do SSM Automation + bucket forense central + OpsCenter. Achados do Config corrigidos por remediação automática com runbook, ID do recurso como parâmetro e AutomationAssumeRole. Aprovação humana dentro do runbook: aws:approve (Approvers, MinRequiredApprovals, SNS com prefixo Automation).

Step Functions para fluxos com espera humana

Aprovação humana no meio do fluxo: Standard com .waitForTaskToken. Express não espera callback.

Security Hub CSPM automation rules e OpsCenter

Mudar severidade ou suprimir achados por critério, sem código: automation rules na conta administradora. Achados viram itens de trabalho com runbooks no Systems Manager OpsCenter integrado ao Security Hub CSPM.

Preparação multi-conta

Role de resposta pronta em toda a organização, inclusive contas futuras: StackSet service-managed com auto-deploy, assumida a partir de conta de segurança ou forense.
OrganizationAccountAccessRole tem acesso total e exige partir da conta de gerenciamento. Uma conta por carga e ambiente reduz o raio de impacto; VPC separa rede, não IAM.

Shield Advanced e SRT

Para a SRT ligar durante o ataque: proactive engagement, que depende de health checks do Route 53 associados aos recursos protegidos e só é acionado por eventos detectados pelo Shield Advanced. A role com AWSShieldDRTAccessPolicy permite à SRT atuar quando você abre chamado. Preparação para DDoS L7: grupo Anti-DDoS no web ACL.

Testes do plano de resposta

Processo e pessoas, sem ferramentas: tabletop. Detecção com ataque simulado: purple ou red team. Condição real com freio automático: AWS FIS com stop condition em alarme do CloudWatch. Metas de RTO e RPO avaliadas contra a arquitetura com recomendações: AWS Resilience Hub.

Root de conta membro comprometido

Excluir as credenciais pelo acesso root centralizado e investigar os eventos Root no CloudTrail; não feche nem remova a conta. Notificações de segurança da AWS chegam ao time certo pelo contato alternativo SECURITY, definido centralmente com PutAlternateContact.

Macetes para memorizar

Ordem forense
Fotografa a configuração antes de mexer, isola sem desligar, memória antes do disco, recria de AMI confiável.

Credencial vazada
CIR: Conter, Investigar, Rotacionar. Excluir só no fim.

Reversível primeiro
Desabilitar volta; excluir não volta. Na dúvida, Disable.

Sessão já emitida
Trust policy fecha a porta da frente; quem já entrou sai só com TokenIssueTime.

Auto Scaling
Tira do grupo antes de tirar da rede.

Quem e como era
CloudTrail diz QUEM; Config diz COMO ERA.

Tabela de memorização: não confunda

Quando é...	...e quando é
DisableKey Contenção reversível e imediata quando há dúvida.	**ScheduleKeyDeletion** Só quando há certeza de que nada mais depende da chave; após 7 a 30 dias é permanente.
Trocar security group Isolar novas conexões e manter a instância para perícia.	**Deny na NACL** Cortar na hora uma conexão já rastreada que o SG não derruba.
Amazon Detective Investigar escopo e causa raiz com grafos prontos, a partir de quando foi habilitado.	**Athena sobre logs no S3** Linha do tempo com histórico anterior ou consultas próprias.
Step Functions Standard Fluxo com espera de horas por aprovação (.waitForTaskToken).	**Step Functions Express** Fluxos curtos sem callback.
Routing control + safety rules do ARC Failover entre Regiões controlado por humano, sem depender do plano de controle.	**Zonal shift** Deslocar tráfego entre zonas de disponibilidade da mesma Região.
AWS FIS Injetar falhas e testar comportamento com stop condition.	**AWS Resilience Hub** Avaliar RTO e RPO contra a arquitetura real e gerar recomendações.
Tabletop Validar processo, papéis e pessoas sem ferramentas.	**Red team** Testar a detecção sem aviso, depois que processos já foram validados.

Números que caem

Item	Valor
Janela de recuperação de segredo excluído (DeleteSecret)	**7 a 30 dias, padrão 30**
Timeout de aws:approve no SSM Automation	**padrão de 7 dias, máximo de 30 dias**
Concorrência reservada para parar uma Lambda	**0**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Alterar a trust policy ou o instance profile para invalidar a credencial roubada.
Como não cair: Isso afeta só novas chamadas AssumeRole; sessões emitidas seguem válidas. Revogue com aws:TokenIssueTime.

⚠ **Alerta de prova:** Encerrar ou parar a instância comprometida para conter rápido.
Como não cair: Perde memória volátil e pode apagar volumes; colete memória e snapshot primeiro.

⚠ **Alerta de prova:** Confiar em termination protection ou scale-in protection em instância de ASG.
Como não cair: Nenhum dos dois impede a substituição por health check; desanexe ou coloque em Standby.

⚠ **Alerta de prova:** Bloquear o IP do atacante na NACL da origem atrás do CloudFront.
Como não cair: A origem só vê IPs da borda do CloudFront; use IP set no escopo Global em regra Block da web ACL.

⚠ **Alerta de prova:** Usar IP set regional na web ACL do CloudFront.
Como não cair: Web ACL do CloudFront exige IP set no escopo Global (CloudFront).

⚠ **Alerta de prova:** Adicionar o IP privado do scanner à trusted list do GuardDuty.
Como não cair: Listas de IPs confiáveis valem só para IPs públicos; use suppression rule com tipo do finding + image ID ou tag.

⚠ **Alerta de prova:** Rotacionar a chave KMS para cortar o acesso de uma conta desconhecida.
Como não cair: A rotação mantém as versões antigas da chave para decifrar; o acesso vem da key policy, que é o que deve ser corrigido.

⚠ **Alerta de prova:** Usar DeleteImportedKeyMaterial em chave com material gerado pelo KMS.
Como não cair: Só se aplica a chaves de origem EXTERNAL; na chave comum, a contenção reversível é DisableKey.

⚠ **Alerta de prova:** Restaurar o banco a partir do snapshot da madrugada e apagar a instância adulterada.
Como não cair: Point-in-time restore em instância nova até o momento antes da adulteração; a original fica isolada para perícia.

⚠ **Alerta de prova:** Suspender o versionamento ou apagar a versão maliciosa após ransomware no S3.
Como não cair: Copie a versão boa por cima e preserve a maliciosa como evidência.

⚠ **Alerta de prova:** Filtrar os findings do GuardDuty pelo IP malicioso (remoteIpDetails) para delimitar o escopo.
Como não cair: O filtro mostra só os recursos que geraram finding; quem trocou tráfego com o IP sem finding fica de fora. Use o perfil de entidade do IP no Amazon Detective.

⚠ **Alerta de prova:** Usar Network Access Analyzer para saber com quem o IP malicioso se comunicou.
Como não cair: Ele mostra caminhos possíveis pela configuração, não comunicações que aconteceram.

⚠ **Alerta de prova:** Deixar o Cognito threat protection em modo audit-only contra credential stuffing.
Como não cair: Audit-only só registra; a resposta exige full function no plano Plus.

⚠ **Alerta de prova:** Fazer drain e encerrar o nó EKS comprometido para limpar o cluster.
Como não cair: Contenha com cordon e network policy, proteja contra encerramento, capture memória e depois snapshot.

Como cai na prova

📝 **Como cai:** Lista de ações para uma EC2 comprometida, às vezes em ordenação.
Como resolver: Metadados antes de mudar security group, role ou tags; se estiver em ASG, desanexe primeiro; isolar com security group de quarentena não apaga memória nem disco; parar ou encerrar só depois da memória e do snapshot; recrie de AMI confiável.

📝 **Como cai:** Credencial ou sessão comprometida que 'continua funcionando' depois da correção.
Como resolver: Identifique o tipo: sessão temporária pede revogação por aws:TokenIssueTime; chave de usuário IAM pede Inactive + Deny; conexão de rede pede NACL.

📝 **Como cai:** Resposta automatizada com menor esforço e auditoria.
Como resolver: Prefira EventBridge + SSM Automation (com aws:approve se exigir humano), remediação automática do Config e automation rules do Security Hub CSPM; descarte Lambda e scripts próprios quando há recurso nativo.

📝 **Como cai:** Investigação: escopo, causa raiz ou linha do tempo.
Como resolver: Detective para entidade e histórico do principal (se já habilitado); Athena para logs já no S3; Config timeline para 'como era'; CloudTrail para 'quem chamou'.

📝 **Como cai:** Preparação antes do incidente.
Como resolver: Role de resposta via StackSets service-managed com auto-deploy, conta por carga, contatos SECURITY, testes por tabletop, FIS ou Resilience Hub conforme o objetivo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
quem mais falou com este IP	**Perfil de entidade de IP no Amazon Detective**
verificar malware em EC2 sem agente e sem achado do GuardDuty	**On-demand malware scan do GuardDuty pelo ARN da instância**
sessão do atacante continua depois de trocar o SG	**Rastreamento de conexão; Deny na NACL**
parar uma Lambda sem destruir evidência	**Concorrência reservada 0**
aprovação de analista que pode levar horas	**Step Functions Standard com .waitForTaskToken ou aws:approve no SSM Automation**
falso positivo validado de scanner autorizado	**Suppression rule no administrador com tipo do finding + image ID ou tag**
exposição pública passada sem eventos de dados no trail	**Server access logs do S3 como prova; Block Public Access para conter sem apagar a política**
credential stuffing no Cognito	**Threat protection no plano Plus em full function**
SRT ligando para você durante o ataque	**Proactive engagement com health checks do Route 53**
playbook de investigação interativo e reprodutível	**Notebook do SageMaker AI**
recuperar banco ao momento antes da adulteração preservando evidência	**Point-in-time restore em instância nova**

role comprometida em várias contas	**SCP negando a role, quarentena por security group, logs protegidos e coleta central**
notificações de segurança da AWS chegando à pessoa errada	**Contato alternativo SECURITY via PutAlternateContact**

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

- Coletar antes de alterar: nunca encerre, apague ou pare antes de memória e snapshot.
- Mudar trust policy não derruba sessões já emitidas; use aws:TokenIssueTime.
- Trocar security group não corta conexão rastreada; NACL Deny corta.
- Desanexe do Auto Scaling group antes de isolar.
- Prefira a contenção reversível (DisableKey, Inactive, concorrência 0).

Essenciais para a prova (checklist)

- ☐ Sei a ordem forense em EC2, EKS e Lambda sem destruir evidência.
- ☐ Sei revogar sessões ativas de uma role com aws:TokenIssueTime.
- ☐ Sei por que trocar security group não encerra conexão existente.
- ☐ Sei conter uma chave KMS de forma reversível e quando agendar exclusão.
- ☐ Sei restaurar um segredo excluído e investigar quem leu um segredo.
- ☐ Sei montar resposta automatizada com EventBridge, SSM Automation e aprovação humana.
- ☐ Sei quando usar Detective, Athena, Config timeline e CloudTrail na investigação.
- ☐ Sei preparar acesso de resposta em todas as contas com StackSets service-managed.
- ☐ Sei diferenciar tabletop, red team, FIS e Resilience Hub.

Questões de revisão do capítulo

R2.1 · Domínio 2: Resposta a incidentes

Durante uma investigação, o time de segurança descobriu que uma função AWS Lambda acionada por eventos do Amazon S3 foi usada para exfiltrar dados sensíveis depois que as credenciais de um desenvolvedor foram comprometidas. A função já foi impedida de executar, mas a equipe precisa (1) preservar evidências, (2) reconstruir a linha do tempo da exfiltração e (3) reduzir a chance de reutilização do vetor, mantendo o ambiente o mais próximo possível do estado no momento do ataque. Qual combinação de ações é MAIS adequada?

A. Publicar nova versão da função com código limpo e aplicar permissions boundary na role, analisando os logs depois da correção
B. Clonar a função para uma nova conta, exportar os logs para um bucket forense e aplicar menor privilégio à role da função comprometida durante a coleta
C. Preservar os logs com Object Lock, capturar código, variáveis e role da função e copiar os dados afetados antes de restringir
D. Excluir a função e recriá-la com novo nome após rotacionar as credenciais do desenvolvedor, exportando os logs do CloudWatch depois

R2.2 · Domínio 2: Resposta a incidentes

Uma instância comprometida em produção usa um volume EBS criptografado com uma chave KMS gerenciada pelo cliente da conta de produção. A equipe forense trabalha em uma conta separada e precisa de uma cópia do snapshot sob seu controle, criptografada com a chave da própria conta forense, sem dar à conta forense acesso a outros dados de produção. Qual solução atende a esses requisitos?

A. Criar o snapshot com a chave aws/ebs da conta de produção e compartilhá-lo com a conta forense, que o copia com a sua própria chave KMS
B. Criar o snapshot, compartilhar a chave KMS por meio de um alias acessível à conta forense e executar CopySnapshot na conta de produção indicando a conta forense como destino da cópia criptografada
C. Compartilhar o snapshot com a conta forense, conceder na key policy à role forense kms:Decrypt, kms:DescribeKey, kms:CreateGrant e kms:ReEncrypt*, e copiar o snapshot com a chave forense
D. Criar uma SCP na OU forense que permita kms:Decrypt na chave de produção e restaurar o volume diretamente do snapshot na conta forense

R2.3 · Domínio 2: Resposta a incidentes

Uma instância de um Auto Scaling group atrás de um Application Load Balancer gerou o finding Backdoor:EC2/C&CActivity.B. O runbook manda trocar o security group da instância por um de quarentena sem regras e coletar memória e disco. No último incidente, minutos depois da troca, o Auto Scaling group encerrou a instância por falha no health check do ELB e a memória se perdeu. Qual ação deve ser executada antes de isolar a instância para preservar a evidência sem reduzir a capacidade do serviço?

A. Habilitar a proteção contra encerramento do EC2 (DisableApiTermination) na instância e depois aplicar o security group de quarentena
B. Habilitar na instância a proteção contra scale-in do Auto Scaling group e depois aplicar o security group de quarentena e coletar as evidências
C. Desanexar a instância do Auto Scaling group sem reduzir a capacidade desejada, para que o grupo lance uma substituta, e depois isolar e coletar
D. Criar snapshots dos volumes EBS, aplicar o security group de quarentena e deixar o Auto Scaling group substituir a instância quando ela falhar

R2.4 · Domínio 2: Resposta a incidentes

Uma seguradora usa o Amazon GuardDuty com administrador delegado na conta Security. Toda segunda-feira surgem findings Recon:EC2/Portscan apontando para instâncias criadas a partir da AMI ami-0a1b2c3d do scanner de vulnerabilidades interno, que varre as sub-redes privadas pelos IPs privados. O analista confirmou pela agenda do scanner, pela tag e pelo registro de mudança que a atividade é autorizada. A equipe quer parar de receber esses findings no Security Hub CSPM e no SIEM sem perder a detecção de varreduras feitas por qualquer outra instância. Qual ação atende ao requisito?

A. Adicionar os IPs privados das instâncias do scanner a uma lista de IPs confiáveis do GuardDuty na conta Security e ativar a lista em cada Região usada
B. Criar na conta Security uma regra de supressão para o tipo Recon:EC2/Portscan, já que a varredura de portas interna é atividade esperada no ambiente
C. Criar na conta Security uma regra de supressão com o tipo Recon:EC2/Portscan e o atributo Instance image ID igual à AMI do scanner
D. Criar na conta membro que hospeda o scanner uma regra de supressão com o tipo Recon:EC2/Portscan e o atributo Instance image ID igual à AMI

Respostas comentadas

R2.1. C) Preservar os logs com Object Lock, capturar código, variáveis e role da função e copiar os dados afetados antes de restringir

Por quê: Na resposta a incidentes, a coleta vem antes da erradicação: os logs do CloudTrail e do CloudWatch Logs vão para um bucket com S3 Object Lock, o pacote de código, as variáveis de ambiente, a política de recurso e a role são capturados (por exemplo, com GetFunction e GetPolicy) e os objetos afetados são copiados para a conta de segurança. Só depois a role é restringida e a função corrigida, preservando a cadeia de custódia.

✗ A) Incorreta. Publicar nova versão e mudar a role antes de coletar altera o estado do ambiente e prejudica a reconstrução.
✗ B) Incorreta. A cópia em outra conta muda ARNs e integrações, e alterar a role durante a coleta modifica o objeto em análise.
✗ D) Incorreta. Excluir a função destrói código, configuração e versões, que são evidência do incidente.

> **Dica de prova:** Incidente com Lambda: coletar código, configuração e logs imutáveis antes de corrigir.

R2.2. C) Compartilhar o snapshot com a conta forense, conceder na key policy à role forense kms:Decrypt, kms:DescribeKey, kms:CreateGrant e kms:ReEncrypt*, e copiar o snapshot com a chave forense

Por quê: Snapshots EBS criptografados só podem ser compartilhados se usarem chave gerenciada pelo cliente. A conta de origem altera as permissões do snapshot e a key policy; a conta de destino copia o snapshot e pode recriptografá-lo com uma chave própria, ficando independente da chave de origem.

✗ A) Incorreta. Snapshots criptografados com a chave gerenciada pela AWS (aws/ebs) não podem ser compartilhados com outras contas.
✗ B) Incorreta. Aliases não são compartilháveis entre contas, e CopySnapshot é executado pela conta que recebe a cópia, não pela conta de origem.
✗ D) Incorreta. SCPs não concedem permissões, e o acesso entre contas à chave depende da key policy da conta de produção.

> **Dica de prova:** Snapshot criptografado entre contas: chave do cliente (não aws/ebs), permissão no snapshot e na key policy, cópia com a chave de destino.

R2.3. C) Desanexar a instância do Auto Scaling group sem reduzir a capacidade desejada, para que o grupo lance uma substituta, e depois isolar e coletar

Por quê: Instâncias em Auto Scaling groups são substituídas quando falham em health checks, e o isolamento de rede provoca essa falha. Antes de conter, a instância deve sair do controle do grupo, desanexando-a (com ou sem reduzir a capacidade desejada) ou colocando-a em Standby, o que também a remove do target group. A proteção contra encerramento do EC2 e a proteção contra scale-in não evitam a substituição por health check.

✗ A) Incorreta. A proteção contra encerramento do EC2 não impede que o Amazon EC2 Auto Scaling encerre a instância em uma substituição por health check.
✗ B) Incorreta. A proteção contra scale-in impede o encerramento por redução de capacidade, mas não a substituição de instâncias marcadas como não saudáveis.
✗ D) Incorreta. O snapshot preserva os discos, mas a memória volátil se perde quando a instância é encerrada na substituição.

> **Dica de prova:** Forense em instância de Auto Scaling group: primeiro desanexe ou coloque em Standby, depois isole; termination protection do EC2 não segura o Auto Scaling.

R2.4. C) Criar na conta Security uma regra de supressão com o tipo Recon:EC2/Portscan e o atributo Instance image ID igual à AMI do scanner

Por quê: Regras de supressão arquivam automaticamente findings novos que correspondem aos critérios, e esses findings não são enviados ao Security Hub CSPM, ao Detective, ao S3 nem ao EventBridge. O padrão recomendado é combinar o tipo do finding com um atributo que identifique só a origem legítima, como Instance image ID ou tag, e criar a regra na conta administradora.

✗ A) Incorreta. Listas de IPs confiáveis e entity lists do GuardDuty valem só para tráfego com endereços públicos roteáveis; os IPs privados do scanner não seriam considerados.

✗ B) Incorreta. Suprimir o tipo inteiro esconderia varreduras feitas por uma instância comprometida, perdendo a detecção que o requisito manda manter.

✗ D) Incorreta. Os critérios estão certos, mas em ambiente multi-conta só o administrador do GuardDuty pode criar regras de supressão; a conta membro não consegue criá-las.

> **Dica de prova:** Falso positivo validado de scanner autorizado: regra de supressão no administrador com tipo do finding + image ID ou tag. Lista de IPs confiáveis só vale para IP público.

03

CAPÍTULO 3 · 18% DA PROVA

Domínio 3: Segurança de infraestrutura

Aqui eu preciso dominar a proteção de borda (WAF, Shield, CloudFront), a rede (security groups, NACLs, endpoints, PrivateLink, Network Firewall, DNS Firewall, Direct Connect com MACsec) e a proteção de computação (IMDSv2, Session Manager, Inspector, ECS, EKS, Lambda, imagens). A prova adora o detalhe de camada: WAF é L7 e não se associa a NLB nem a Transit Gateway; security group é stateful e NACL é stateless. Também cai muito 'sem internet', 'sem bastion', 'sem agente' e 'sem mudar código', e a resposta é o recurso gerenciado exato. Onde mais erro: portas efêmeras na NACL, gateway endpoint que não é transitivo e trocar a ferramenta de prevenção por uma de detecção.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Security group x NACL

Security group é stateful: o retorno de conexões permitidas passa automaticamente. NACL é stateless e baseada em portas: precisa liberar a saída para portas efêmeras (1024-65535) e avaliar os dois sentidos. Security groups podem referenciar outros SGs (bastion, aplicação, banco); em peering na mesma Região dá para referenciar o SG da VPC emparelhada, entre Regiões só CIDR.

VPC endpoints

Gateway endpoint só existe para S3 e DynamoDB e não é transitivo (on-premises não o usa). Interface endpoint (PrivateLink) com DNS privado leva KMS, Secrets Manager, SSM e outros sem internet e sem mudar código. Endpoint policy com lista de recursos ou aws:ResourceOrgID evita exfiltração para buckets e tabelas de outras contas.

AWS PrivateLink para serviço entre contas

Provedor publica endpoint service atrás de NLB e escolhe os principais; consumidor cria interface endpoint. Tráfego unidirecional, sem internet e sem rotas entre VPCs, por isso CIDR sobreposto não é problema. VPC peering não aceita CIDR sobreposto e cria rotas nos dois sentidos.

AWS WAF

Inspeção L7 em CloudFront (escopo global), ALB, API Gateway REST, AppSync e similares; nunca em NLB, Transit Gateway ou HTTP API. Managed rule groups (Core rule set, Known bad inputs) tratam exploração HTTP sem mudar código. Regra nova: override para Count, analisar logs, depois Block.

Proteções gerenciadas de bots e fraude no WAF

Credential stuffing no login: ATP. Cadastro fraudulento: ACFP. Robôs genéricos: Bot Control; bot que se passa por navegador e gira IP pede Bot Control targeted. Bot que troca de IP mas mantém o cliente TLS: regra por fingerprint JA4/JA3. Challenge verifica o navegador sem atrito; CAPTCHA prova que é humano.

Regras de taxa e geografia no WAF

IP compartilhado por muitos usuários legítimos: combine IP com outra chave (cabeçalho, cookie) e use scope-down na rota sensível. Bloqueio por país com exceção por IP: AND(NOT geo, NOT IP set) ou Allow do IP set antes; restrição geográfica do CloudFront não tem exceção.

Shield Standard x Shield Advanced

Standard é automático, grátis, L3/L4, sem ativação por recurso. Advanced acrescenta SRT, proteção de custos e L7; protection group reduz falso positivo em blue/green, e health check do Route 53 melhora a detecção e é requisito do proactive engagement.

CloudFront: origem protegida e cabeçalhos

Evitar bypass do CloudFront e WAF: ALB interno como VPC origin ou prefix list gerenciado do CloudFront no SG. CloudFront + S3 com SSE-KMS: OAC (não OAI), bucket policy e key policy com cloudfront.amazonaws.com e AWS:SourceArn da distribuição. Response headers policy define cabeçalhos de segurança no navegador; origin request policy é o caminho para a origem. Field-level encryption deixa um campo legível só no destino final.

IMDSv2 contra SSRF

HttpTokens required, hop limit 1 sem contêineres, aplicado em execução e na launch template. Tráfego para 169.254.169.254 não sai pela rede da VPC, então NACL e SG não o filtram.

Acesso administrativo sem portas abertas

Session Manager: sem portas, sem chaves SSH e com registro de sessões; em sub-rede sem internet precisa dos endpoints ssm, ssmmessages e ec2messages. EC2 Instance Connect Endpoint: SSH/RDP em instância privada sem agente e sem bastion. Servidor on-premises no Systems Manager: hybrid activation + SSM Agent, nó com ID mi-.

Direct Connect criptografado

Camada 2 sem perder vazão: MACsec em conexão dedicada (10, 100 e 400 Gbps) e LAGs; não existe em conexão hospedada. Em conexão hospedada ou sem IP público: VPN IPsec de IP privado sobre transit VIF, que criptografa em camada 3 com vazão limitada por túnel.

AWS Network Firewall e inspeção centralizada

Filtro de saída por domínio com SNI, assinatura no payload com regras Suricata e inspeção TLS gerenciada sem agente (sem ela o firewall vê só metadados). Inspeção leste-oeste com Transit Gateway: VPC de inspeção + appliance mode no attachment. Firewalls de terceiros: Gateway Load Balancer.

Route 53 Resolver DNS Firewall

Bloqueia domínio malicioso ou túnel DNS no resolvedor da VPC, com listas gerenciadas e Advanced, em escala com Firewall Manager. Regra detectiva depois da consulta chega tarde.

Amazon Inspector

CVE em EC2, imagens do ECR (varredura contínua reavalia imagens já publicadas; scan básico não) e Lambda (padrão + varredura de código). Network reachability mostra porta exposta + CVE. CIS do sistema operacional por tag e agenda. SBOM Generator + Scan API no build barram imagem antes do push. Inspector Code Security nos repositórios; CodeGuru Security foi descontinuado.

Papéis de execução em ECS e Lambda

ECS: task execution role é o que o agente usa para subir a task (imagem, logs, secrets); task role é o que o código chama. Lambda: execution role controla o que a função faz; política de recurso controla quem invoca. Lambda em VPC sem NAT acessa serviços por VPC endpoints.

Segurança de contêineres

Imagem mínima, usuário não root, readonlyRootFilesystem. Origem e assinatura de imagem: admission controller; privilégio de pod: Pod Security Admission restricted. Segmentar pods: network policies nativas do VPC CNI. Push restrito por IAM, pull por repository policy. GuardDuty Runtime Monitoring em ECS no Fargate usa sidecar automatizado; EKS em Fargate não é suportado.

Network Access Analyzer x Reachability Analyzer

Provar que um segmento inteiro não é alcançável da internet: Network Access Analyzer (pede escopos). Diagnosticar um par origem-destino: Reachability Analyzer. Flow Logs só mostram o que aconteceu, não provam ausência de caminho.

Segurança de IA generativa

Prompt injection e vazamento de PII: Bedrock Guardrails com Prompt Attack e sensitive information filters; conteúdo recuperado deve ser tratado como entrada não confiável. Lista de modelos permitidos: SCP ou IAM negando bedrock:InvokeModel* fora dos ARNs aprovados; guardrails tratam conteúdo, não escolha de modelo.

Macetes para memorizar

💡 Stateful x stateless

SG tem memória; NACL é esquecida: lembre das efêmeras 1024-65535.

💡 Camadas

WAF = 7; SG e NACL = 3 e 4; Shield = DDoS.

💡 Gateway endpoint

Só S3 e Dynamo, e não atravessa ninguém.

💡 Session Manager sem internet

Os três SSM: ssm, ssmmessages, ec2messages.

💡 Bots

ATP no login, ACFP no cadastro, Bot Control no resto; trocou IP mas não o TLS = JA4.

💡 Detecção x CVE

Inspector acha a falha; GuardDuty pega o comportamento.

Tabela de memorização: não confunda

Quando é...	...e quando é
Gateway endpoint S3 e DynamoDB a partir da própria VPC; não é transitivo.	**Interface endpoint** Demais serviços (KMS, Secrets Manager, SSM) e acesso a partir do on-premises.
Session Manager Acesso sem portas e sem chaves, com sessões registradas; exige SSM Agent.	**EC2 Instance Connect Endpoint** SSH/RDP em instância privada sem agente e sem bastion.
MACsec Camada 2 sem perder vazão, em conexão dedicada.	**VPN IPsec sobre Direct Connect** Conexão hospedada ou criptografia em camada 3.
Network Access Analyzer Provar que nenhum caminho da internet alcança um segmento.	**Reachability Analyzer** Diagnosticar a conectividade de um par específico.
Bot Control comum Bots que se identificam ou têm assinatura conhecida.	**Bot Control targeted** Bots que imitam navegador e giram IP.

Task execution role Pull do ECR, awslogs e secrets da task definition.	**Task role** Chamadas que o código da aplicação faz à AWS.
PrivateLink Expor um serviço, CIDR sobreposto, só o consumidor inicia.	**VPC peering** Rede a rede sem sobreposição, rotas nos dois sentidos, não transitivo.

Números que caem

Item	Valor
Portas efêmeras de retorno na NACL	**1024-65535**
Velocidades de conexão dedicada com MACsec	**10, 100 e 400 Gbps**
Endereço do serviço de metadados da instância	**169.254.169.254**
Hop limit do IMDSv2 sem contêineres	**1**
Endpoints de interface do Session Manager	**ssm, ssmmessages e ec2messages**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Associar o AWS WAF a um NLB ou a um Transit Gateway.
Como não cair: WAF se associa a CloudFront, ALB, API Gateway, AppSync e similares; nunca NLB nem TGW.

⚠ **Alerta de prova:** Liberar a entrada na NACL e esquecer o retorno.
Como não cair: NACL é stateless: libere a saída para portas efêmeras 1024-65535; SG já deixa o retorno passar.

⚠ **Alerta de prova:** Bloquear o IMDS com NACL ou security group contra SSRF.
Como não cair: O tráfego para 169.254.169.254 não passa por eles; exija IMDSv2 com hop limit 1.

⚠ **Alerta de prova:** Usar VPC peering com a VPC de inspeção para alcançar outras VPCs ou a internet.
Como não cair: Peering não é transitivo; use Transit Gateway com VPC de inspeção e appliance mode.

⚠ **Alerta de prova:** Usar endpoint FIPS para alcançar o Secrets Manager de Lambda sem internet.
Como não cair: Endpoints FIPS continuam públicos; sem internet, precisa de interface endpoint.

⚠ **Alerta de prova:** Habilitar Shield Standard por recurso.
Como não cair: Shield Standard é automático e sem custo para todos; não há ativação.

⚠ **Alerta de prova:** Limitar taxa por IP contra bot que troca de IP a cada poucas requisições.
Como não cair: Cada IP fica abaixo do limite; use fingerprint JA4/JA3 ou Bot Control targeted.

⚠ **Alerta de prova:** Usar IAM Roles Anywhere ou chave de acesso em EC2.
Como não cair: Em EC2 a forma nativa é instance profile; Roles Anywhere é para servidores fora da AWS.

⚠ **Alerta de prova:** Anexar o SG do bastion às instâncias privadas para restringir a origem.
Como não cair: Referencie o SG do bastion como origem na regra do SG das instâncias.

⚠ **Alerta de prova:** Usar o cabeçalho Referer como controle de segurança.
Como não cair: É facilmente forjado; CORS com AllowedOrigin específico e autorização por política ou URL pré-assinada.

⚠ **Alerta de prova:** Contar com TLS em cada salto para esconder um campo sensível dos microsserviços.
Como não cair: Cada componente que termina TLS lê o corpo; use field-level encryption do CloudFront.

⚠ **Alerta de prova:** Varrer a AMI depois de distribuída às contas de produção.
Como não cair: Teste e endureça antes de distribuir com EC2 Image Builder (componentes de hardening e de teste).

⚠ **Alerta de prova:** Achar que GuardDuty Runtime Monitoring encontra CVEs da imagem.
Como não cair: Ele detecta comportamento em execução; CVE é Amazon Inspector.

⚠ **Alerta de prova:** Usar Network Firewall para filtrar consultas DNS ao Resolver.
Como não cair: Consultas ao Resolver se filtram com Route 53 Resolver DNS Firewall.

Como cai na prova

📝 **Como cai:** Conexão falhando 'mesmo com security groups corretos'.
Como resolver: Olhe NACL nos dois sentidos e portas efêmeras; depois rotas e endpoints. SG é stateful e raramente é a causa do retorno bloqueado.

📝 **Como cai:** Ataque web na borda com exigência de não mudar código.
Como resolver: WAF com managed rule groups no CloudFront ou ALB; teste em Count antes de Block; escolha a proteção específica (ATP, ACFP, Bot Control, fingerprint) pelo tipo de bot.

📝 **Como cai:** Workload sem saída para a internet que precisa de serviços da AWS.
Como resolver: Gateway endpoint para S3 e DynamoDB e interface endpoints com DNS privado para o resto; sem NAT nem rota 0.0.0.0/0; endpoint policy para evitar exfiltração.

📝 **Como cai:** Expor serviço a outra conta ou consumir SaaS com requisitos de isolamento.
Como resolver: Se há CIDR sobreposto ou o provedor não pode ter rota: PrivateLink. Se é rede a rede: peering ou Transit Gateway.

📝 **Como cai:** Escolher a ferramenta de vulnerabilidade ou endurecimento.
Como resolver: CVE em EC2, ECR e Lambda: Inspector; antes do push: SBOM Generator + Scan API; AMI endurecida antes de distribuir: Image Builder; comportamento em execução: GuardDuty.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
camada 2 no Direct Connect sem perder vazão	**MACsec em conexão dedicada**
CIDR sobreposto, sem peering, só o cliente inicia	**PrivateLink (endpoint service + NLB + interface endpoint)**
SSRF contra 169.254.169.254	**IMDSv2 obrigatório, hop limit 1, na launch template**
sem portas abertas, sem chaves SSH, sessões registradas	**Session Manager**
controle L7 entre serviços de várias VPCs sem appliances	**VPC Lattice**
acesso a aplicação interna sem VPN, com postura do dispositivo	**AWS Verified Access**
filtro de saída por domínio	**AWS Network Firewall com SNI**
IPv6 com saída, sem entrada iniciada de fora	**Egress-only internet gateway com rota ::/0**
inspecionar cópia dos pacotes sem mudar rotas	**VPC Traffic Mirroring**
limite de taxa por cliente no API Gateway	**Usage plan + API key**
cada dispositivo IoT só no próprio tópico	**Variável iot:Connection.Thing.ThingName**
mesmas faixas de IP em muitos SGs e contas	**Prefix list gerenciada pelo cliente + AWS RAM**
patch com aprovação atrasada, janela e relatório	**Patch baseline + maintenance window + compliance do Patch Manager**
Client VPN com acesso por grupo do IdP	**Autenticação federada SAML + regras de autorização por Group ID**

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

- WAF não se associa a NLB, Transit Gateway nem HTTP API.
- NACL é stateless: portas efêmeras de saída para o retorno.
- Gateway endpoint: só S3 e DynamoDB, e não é transitivo.
- Chave de acesso dentro de EC2 é sempre resposta errada: use instance profile.
- MACsec só em conexão dedicada; hospedada usa VPN IPsec.

Essenciais para a prova (checklist)

- ☐ Sei diagnosticar bloqueio de NACL e portas efêmeras.
- ☐ Sei escolher entre gateway endpoint, interface endpoint e PrivateLink de serviço.
- ☐ Sei montar proteção L7 com WAF e escolher entre ATP, ACFP, Bot Control e fingerprint.
- ☐ Sei diferenciar Shield Standard e Advanced e o que o proactive engagement exige.
- ☐ Sei proteger a origem do CloudFront com VPC origin, OAC e key policy.
- ☐ Sei exigir IMDSv2 e por que SG e NACL não protegem o IMDS.
- ☐ Sei criptografar Direct Connect com MACsec ou VPN IPsec.
- ☐ Sei centralizar inspeção com Network Firewall, Transit Gateway e appliance mode.
- ☐ Sei separar task execution role de task role e execution role de política de recurso no Lambda.
- ☐ Sei usar Inspector, Image Builder e admission controller na cadeia de imagens.

Questões de revisão do capítulo

R3.1 · Domínio 3: Segurança de infraestrutura

Um hospital mantém 300 servidores Linux e Windows no data center, ligados à AWS por Direct Connect, e já usa o AWS Systems Manager para corrigir suas instâncias EC2. A auditoria exige o mesmo processo para os servidores locais: inventário de software, aplicação mensal de patches pelas mesmas patch baselines e relatório central de conformidade. A equipe não quer abrir portas de entrada no data center nem migrar os servidores. Qual solução atende a esses requisitos?

A. Exportar os servidores para AMIs com o VM Import/Export e usar o EC2 Image Builder para gerar imagens corrigidas todo mês, recriando os servidores a partir delas
B. Instalar o agente do CloudWatch com credenciais de um usuário IAM e criar regras personalizadas do AWS Config que registrem os pacotes instalados e os patches pendentes
C. Criar uma service role com confiança em ssm.amazonaws.com e uma hybrid activation, instalar o SSM Agent com o código e o ID de ativação e usar Patch Manager e Inventory
D. Ativar o Amazon Inspector com varredura baseada em agente nos servidores locais e usar a correção automática de pacotes vulneráveis que o Inspector aplica a cada achado gerado

R3.2 · Domínio 3: Segurança de infraestrutura

Um site de venda de ingressos protege a página de compra com uma regra do AWS WAF que aplica a ação CAPTCHA às requisições de navegadores rotulados como suspeitos pelo Bot Control. Bots simples foram contidos, mas a taxa de conversão caiu porque muitos compradores legítimos desistem diante do quebra-cabeça. A equipe quer continuar verificando que o cliente é um navegador real, sem exigir interação do usuário, e deixar o quebra-cabeça só para os sinais de maior confiança. Qual mudança atende a esse requisito?

A. Manter a ação CAPTCHA na regra e aumentar o tempo de imunidade do CAPTCHA na web ACL, para que cada comprador resolva o quebra-cabeça menos vezes por sessão
B. Mudar a ação da regra para Challenge e criar outra regra com ação CAPTCHA só para os rótulos de bot de maior confiança
C. Mudar a ação da regra para Count com um rótulo próprio e analisar depois os logs do AWS WAF para bloquear os clientes que se comportarem como bots
D. Mudar a ação da regra para Block com uma resposta personalizada que oriente o comprador a tentar novamente em outro navegador ou dispositivo

R3.3 · Domínio 3: Segurança de infraestrutura

Uma distribuidora de energia tem 400 instâncias EC2 com Windows Server e Amazon Linux gerenciadas pelo Systems Manager. A política de segurança exige que atualizações classificadas como críticas e importantes sejam instaladas sete dias após a publicação, somente nas madrugadas de domingo para não afetar a operação, e que a área de conformidade receba relatórios de quais instâncias estão sem patches. Qual solução atende a esses requisitos?

A. Configurar um pipeline do EC2 Image Builder que gere AMIs atualizadas toda semana e substituir as instâncias por meio da equipe de operações a cada nova versão
B. Criar uma associação do State Manager com AWS-RunPatchBaseline na operação Install a cada 30 minutos, usando a baseline padrão da AWS para cada sistema operacional
C. Habilitar o Amazon Inspector nas instâncias e configurar uma regra do EventBridge que, a cada achado de CVE crítica ou importante, execute o AWS-RunPatchBaseline com a operação Install na instância afetada
D. Criar baselines de patches personalizadas com aprovação automática após sete dias para críticas e importantes, uma janela de manutenção aos domingos com AWS-RunPatchBaseline (Install) e relatórios de conformidade

R3.4 · Domínio 3: Segurança de infraestrutura

Uma operadora logística liga o data center às VPCs por uma conexão hospedada (hosted connection) de 1 Gbps do AWS Direct Connect, contratada com um parceiro, usando uma transit VIF associada a um transit gateway. Uma nova norma exige criptografar todo o tráfego híbrido, de qualquer protocolo, e proíbe que o túnel use endereços IP públicos. Qual solução atende a esses requisitos?

A. Habilitar MACsec na conexão hospedada, associando uma CKN e uma CAK ao Direct Connect e ao roteador do data center para criptografar os quadros na camada 2
B. Criar uma AWS Site-to-Site VPN pela internet com o transit gateway e anunciar as rotas on-premises com AS path maior que o da conexão Direct Connect
C. Criar uma AWS Site-to-Site VPN com IP privado sobre a transit VIF, terminando no transit gateway, para levar o tráfego em túneis IPsec
D. Configurar TLS nas aplicações que trafegam pela conexão e exigir políticas de segurança TLS 1.2 nos load balancers internos das VPCs

Respostas comentadas

R3.1. C) Criar uma service role com confiança em ssm.amazonaws.com e uma hybrid activation, instalar o SSM Agent com o código e o ID de ativação e usar Patch Manager e Inventory

Por quê: Para gerenciar máquinas fora da AWS com o Systems Manager, cria-se uma hybrid activation associada a uma IAM service role que confia em ssm.amazonaws.com. O SSM Agent instalado com o código e o ID de ativação registra o servidor como managed node com ID iniciado por mi-, usando apenas tráfego de saída. A ativação tem prazo de validade para novos registros, mas não afeta os nós já registrados.

✗ A) Incorreta. A abordagem obriga a migrar e recriar os servidores na AWS, o que contraria a restrição de manter as máquinas no data center.

✗ B) Incorreta. O agente do CloudWatch coleta métricas e logs; o AWS Config não avalia servidores locais dessa forma e nenhum dos dois aplica patches, além de exigir chave de acesso de longo prazo.

✗ D) Incorreta. O Amazon Inspector avalia instâncias EC2, imagens no ECR e funções Lambda; ele não registra servidores locais e não aplica patches, apenas gera achados.

> **Dica de prova:** Servidor on-premises no Systems Manager: hybrid activation + SSM Agent; o nó aparece com ID mi-.

R3.2. B) Mudar a ação da regra para Challenge e criar outra regra com ação CAPTCHA só para os rótulos de bot de maior confiança

Por quê: No AWS WAF, CAPTCHA exige que a pessoa resolva um quebra-cabeça, enquanto Challenge executa um desafio silencioso que verifica se a sessão vem de um navegador, sem envolver o usuário. As duas ações geram um token com tempo de imunidade configurável e só funcionam em navegadores acessando endpoints HTTPS. Uma estratégia comum é usar Challenge para sinais de risco moderado e CAPTCHA quando o Block barraria muitos legítimos.

✗ A) Incorreta. Um tempo de imunidade maior reduz repetições, mas todo comprador novo ainda precisa resolver o quebra-cabeça, mantendo o atrito na primeira compra.

✗ C) Incorreta. Count apenas registra e rotula; os bots passariam livremente até alguém analisar os logs.

✗ D) Incorreta. Bloquear derruba também os compradores legítimos rotulados como suspeitos, piorando a conversão em vez de melhorar.

> **Dica de prova:** Verificar navegador sem atrito: Challenge (silencioso). Provar que é humano: CAPTCHA.

R3.3. D) Criar baselines de patches personalizadas com aprovação automática após sete dias para críticas e importantes, uma janela de manutenção aos domingos com AWS-RunPatchBaseline (Install) e relatórios de conformidade

Por quê: No Patch Manager, a patch baseline define quais atualizações são aprovadas (classificação, severidade e dias de atraso após a publicação), a janela de manutenção controla quando a instalação ocorre e os dados de conformidade mostram quais nós estão sem patches, podendo ser exportados em relatórios. É a combinação típica para atender política de patches com janela controlada.

✗ A) Incorreta. Recriar AMIs é uma boa prática para frotas imutáveis, mas substituir 400 instâncias à mão não garante a janela nem gera relatórios de conformidade de patches.

✗ B) Incorreta. Uma associação a cada 30 minutos instala patches a qualquer hora, desrespeitando a janela, e a baseline padrão não aplica o atraso de sete dias definido pela política.

✗ C) Incorreta. O Inspector detecta vulnerabilidades, mas disparar a instalação a cada achado ignora a janela de domingo e o atraso de sete dias exigidos.

> **Dica de prova:** Patch com atraso de aprovação, horário controlado e relatório: patch baseline + maintenance window + compliance do Patch Manager.

R3.4. C) Criar uma AWS Site-to-Site VPN com IP privado sobre a transit VIF, terminando no transit gateway, para levar o tráfego em túneis IPsec

Por quê: A Private IP VPN permite implantar Site-to-Site VPN IPsec sobre o Direct Connect usando endereços IP privados, com transit VIF e transit gateway. MACsec criptografa na camada 2, mas só em conexões dedicadas suportadas, não em hosted connections.

✗ A) Incorreta. MACsec é suportado em conexões dedicadas (10, 100 e 400 Gbps) e LAGs; não está disponível em conexões hospedadas.

✗ B) Incorreta. Uma VPN pela internet usa endereços públicos nos túneis, e o AS path mais longo faria o tráfego preferir o Direct Connect sem criptografia.

✗ D) Incorreta. TLS nas aplicações não cobre todo o tráfego de qualquer protocolo e depende de cada aplicação; não atende ao requisito de criptografar o tráfego híbrido como um todo.

> **Dica de prova:** Criptografar Direct Connect: MACsec em conexão dedicada; em conexão hospedada ou sem IP público, VPN IPsec de IP privado sobre transit VIF.

04

CAPÍTULO 4 · 20% DA PROVA

Domínio 4: Gerenciamento de identidade e acesso

É o domínio de maior peso, e aqui eu preciso ler políticas como o avaliador do IAM: identidade, permissions boundary, session policy, SCP, RCP e políticas de recurso, com o Deny explícito vencendo tudo. A prova traz mensagens de erro reais (AccessDenied, 1 hour session limit, Response signature invalid, Encoded authorization failure message) e pede a causa exata. Também cai muito a escolha da chave de condição certa (aws:PrincipalOrgID, aws:ResourceOrgID, aws:SourceVpce, aws:CalledVia, iam:PassedToService) e o desenho de federação com IAM Identity Center, SAML, SCIM, Cognito e OIDC. Onde mais erro: achar que SCP concede permissão, esquecer que role chaining limita a 1 hora e usar aws:SourceIp com tráfego que passa por VPC endpoint.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Lógica de avaliação de políticas

Para a ação passar, todas as camadas aplicáveis precisam permitir: identidade E boundary E session policy E SCP; um Deny explícito em qualquer uma bloqueia. SCPs não concedem permissões, só limitam o máximo. Mensagem 'explicit deny in a resource-based policy': nenhum Allow resolve, ajuste a condição do Deny.

Session policy

Passada no AssumeRole, restringe só aquela sessão por interseção com a política da role; nunca amplia. Permissions boundary vale para todas as sessões da role.

Duração de sessão e role chaining

DurationSeconds maior que a MaxSessionDuration configurada na role gera o erro 'exceeds the MaxSessionDuration'; a correção é aumentar a duração máxima da role, que vai até 12 horas. Encadeamento de roles (credenciais de uma role assumindo outra) limita a sessão a 1 hora, independentemente da configuração; não adianta aumentar MaxSessionDuration.

Acesso entre contas

Role na conta de destino com trust policy para o principal de origem + sts:AssumeRole na política de identidade. Terceiro acessando sua conta: role com ExternalId. Principal com :root da outra conta delega ao IAM dela; para uma role só, coloque o ARN. Ler na conta B e gravar na conta A com a mesma credencial pede política de recurso, não AssumeRole (que abre mão das permissões originais).

Chaves de condição de organização

aws:PrincipalOrgID libera recurso a toda a organização sem listar contas; aws:PrincipalOrgPaths restringe a OUs. aws:ResourceOrgID em SCP ou endpoint policy impede que suas identidades usem recursos de fora. aws:SourceOrgID identifica a organização do recurso de origem em chamadas de principais de serviço.

SCP x RCP x política de recurso

SCP limita o que os principais da sua organização fazem. RCP ou política de recurso com aws:PrincipalOrgID limita quem de fora usa seus recursos. Nenhuma das duas alcança credencial e recurso de fora da organização; para exfiltração pela VPC use endpoint policy com aws:ResourceOrgID. SCP não alcança service-linked roles nem a conta de gerenciamento.

Condições de serviço intermediário

kms:ViaService (servico.Região.amazonaws.com) torna a chave usável só por um serviço. aws:CalledVia exige um serviço específico chamando em seu nome; aws:ViaAWSService vale para qualquer serviço. Deny por organização quebrando entrega de logs: acrescente aws:PrincipalIsAWSService false. Service principal em política de recurso: restrinja com aws:SourceArn e aws:SourceAccount juntos.

iam:PassRole e Lambda

'Role cannot be assumed by Lambda' = trust policy sem lambda.amazonaws.com. Erro de iam:PassRole = falta permissão para quem faz o deploy. Limitar para qual serviço a role é passada: iam:PassedToService; iam:AWSServiceName é de service-linked role.

Delegação segura com permissions boundary

Permitir iam:CreateRole condicionado a iam:PermissionsBoundary + Deny em DeleteRolePermissionsBoundary e na edição do boundary evita escalonamento. IAM path no ARN delega administração de um grupo de roles sem prefixo de nome.

ABAC

Comparar aws:PrincipalTag com aws:ResourceTag. Com AssumeRole: session tags + sts:TagSession na trust policy; com Identity Center: attributes for access control. Tag obrigatória na criação: aws:RequestTag com Null; chaves aceitas: aws:TagKeys; recurso existente: aws:ResourceTag.

IAM Identity Center

Permission sets por função, grupos do IdP e atribuições automatizadas. Duração da sessão do portal (padrão 8 horas, de 15 minutos a 90 dias) é diferente da session duration do permission set (padrão 1 hora, máximo 12). Mudou o permission set: reprovisionar; nunca edite as roles AWSReservedSSO. SAML autentica, SCIM provisiona e desprovisiona; grupo aninhado do Entra ID não é provisionado. MFA resistente a phishing: só FIDO2.

Federação SAML no IAM

Atributo Role mapeado para roles do IAM dá permissão por grupo do diretório. 'Response signature invalid' após troca de certificado no IdP: atualizar os metadados SAML no identity provider do IAM. MFA do IdP externo não aparece em aws:MultiFactorAuthPresent: use session tags na asserção.

Credenciais sem chave de longo prazo

EC2: instance profile. Servidor fora da AWS com PKI própria: IAM Roles Anywhere (trust anchor + profile + role). GitHub Actions: OIDC + AssumeRoleWithWebIdentity com condição no claim sub. Pod do EKS: EKS Pod Identity, com IMDSv2 hop limit 1 para esconder a role do nó. Desenvolvedores: Identity Center + aws configure sso.

Amazon Cognito

User pool autentica; identity pool entrega credenciais AWS temporárias (inclusive a visitantes não autenticados, com role de convidado mínima). Token em REST API sem código: authorizer do Cognito; com authorization scopes o método exige token de acesso. Credencial vazada e MFA por risco: threat protection no plano Plus.

IAM Access Analyzer

Acesso externo: recursos compartilhados fora da zona de confiança (corrija a política ou arquive se esperado). Acesso interno: quem dentro da organização acessa recurso crítico. Acesso não utilizado: roles, chaves e permissões ociosas. Validação de políticas (ERROR, SECURITY_WARNING, WARNING, SUGGESTION) e verificações personalizadas no pipeline; geração de política a partir do trail do CloudTrail.

MFA para usuários IAM

Deny com BoolIfExists aws:MultiFactorAuthPresent false e exceção para gerenciar o próprio MFA. Na CLI: get-session-token com --serial-number e --token-code.

Diagnóstico de negação

Encoded authorization failure message: sts decode-authorization-message (permissão sts:DecodeAuthorizationMessage). IAM policy simulator em modo principal inclui boundary e SCP, não RCP. ConsoleLogin Failure com Failed authentication é senha ou MFA, não política. Trust policy com AROA... no Principal: a role foi recriada.

Autorização dentro da aplicação

Regras de quem vê qual registro, externas ao código: Amazon Verified Permissions com Cedar. Linhas do DynamoDB por usuário: dynamodb:LeadingKeys; dynamodb:Attributes limita colunas.

Macetes para memorizar

Avaliação

Deny explícito > Allow > deny implícito. Todas as camadas precisam dizer sim.

SCP

SCP é cerca, não chave: limita, nunca dá.

Org IDs

PrincipalOrgID protege o MEU recurso de quem é de fora; ResourceOrgID impede o MEU principal de ir para fora.

Role chaining

Role puxando role = uma hora e acabou.

Cognito

User pool diz QUEM é; identity pool dá a CHAVE da AWS.

Federação

SAML entra, SCIM cadastra.

Rotação de access key

Cria, troca, confere last used, inativa, exclui.

Tabela de memorização: não confunda

Quando é...	...e quando é
SCP Limitar o que identidades da sua organização fazem (inclusive usar recursos de fora com aws:ResourceOrgID).	**RCP** Limitar o acesso aos seus recursos por identidades de fora (perímetro de dados).
Session policy Restringir uma sessão específica sem mudar a role.	**Permissions boundary** Teto permanente para todas as sessões da identidade, inclusive em delegação.
aws:CalledVia Exigir que um serviço específico (ex.: Athena) chame em seu nome.	**aws:ViaAWSService** Aceitar qualquer serviço chamando com suas credenciais.

User pool do Cognito Autenticar usuários da aplicação e emitir tokens.	**Identity pool do Cognito** Trocar identidade por credenciais AWS temporárias.
Authorizer do Cognito Token de user pool em REST API sem código.	**Lambda authorizer** Lógica própria ou outro IdP.
Duração da sessão do portal do Identity Center Quanto tempo até reautenticar no portal.	**Session duration do permission set** Quanto tempo dura a sessão dentro de cada conta.
aws:SourceVpce Restringir a acesso vindo de um VPC endpoint.	**aws:SourceIp** IPs públicos; some do contexto quando a chamada passa por VPC endpoint.

Números que caem

Item	Valor
MaxSessionDuration de uma role	**até 12 horas**
Sessão em role chaining	**máximo de 1 hora**
Session duration do permission set	**padrão de 1 hora, máximo de 12**
Sessão do portal do IAM Identity Center	**padrão de 8 horas, de 15 minutos a 90 dias**
Validade máxima de URL pré-assinada com SigV4	**7 dias**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Criar uma SCP com Allow para dar acesso que está faltando.
Como não cair: SCP não concede permissão; sem Allow na política de identidade continua negado.

⚠ **Alerta de prova:** Aumentar MaxSessionDuration para resolver o '1 hour session limit'.
Como não cair: É role chaining, limitado a 1 hora independentemente da configuração; renove a sessão.

⚠ **Alerta de prova:** Usar aws:SourceIp com IP privado ou depois de adotar VPC endpoint.
Como não cair: A chave some do contexto via endpoint; use aws:SourceVpce no mesmo Deny.

⚠ **Alerta de prova:** Usar aws:ViaAWSService para liberar só o Athena.
Como não cair: É verdadeira para qualquer serviço; para um serviço específico, aws:CalledVia.

⚠ **Alerta de prova:** Usar aws:CalledVia para restringir o uso da chave KMS ao RDS.
Como não cair: CalledVia só é preenchida por alguns serviços; para KMS, kms:ViaService.

⚠ **Alerta de prova:** Usar dynamodb:Attributes para que cada usuário veja só seus itens.
Como não cair: Attributes limita colunas; linhas por usuário pedem dynamodb:LeadingKeys.

⚠ **Alerta de prova:** Bloquear exfiltração para bucket de terceiros com SCP ou RCP.
Como não cair: Elas não alcançam credencial e recurso de fora; use endpoint policy com aws:ResourceOrgID.

⚠ **Alerta de prova:** Editar direto a role AWSReservedSSO ou esperar cache expirar após mudar o permission set.
Como não cair: A role tem a política antiga até reprovisionar o permission set.

⚠ **Alerta de prova:** Usar ${aws:username} em pasta pessoal de usuários federados.
Como não cair: Só vale para usuário IAM; use ${aws:PrincipalTag/...} vindo de session tags.

⚠ **Alerta de prova:** Usar iam:AWSServiceName para limitar para qual serviço a role é passada.
Como não cair: Essa chave é de service-linked role; a certa é iam:PassedToService.

⚠ **Alerta de prova:** Arquivar um achado de acesso externo não autorizado.
Como não cair: Arquivar esconde; corrija a política. Regra de arquivamento é para acesso esperado.

⚠ **Alerta de prova:** Usar AD Connector para RDS for SQL Server com autenticação do Windows.
Como não cair: Só AWS Managed Microsoft AD, com trust para o AD local.

⚠ **Alerta de prova:** Compartilhar bucket do S3 por AWS RAM.
Como não cair: RAM não compartilha buckets; use role ou bucket policy.

⚠ **Alerta de prova:** Tratar AccessDenied entre contas só olhando a bucket policy.
Como não cair: A política de identidade do chamador também precisa citar o recurso da outra conta.

Como cai na prova

📝 **Como cai:** Mensagem de erro literal e pergunta da causa.
Como resolver: Classifique: autenticação (Failed authentication, signature invalid) x autorização (AccessDenied, explicit deny) x limite de sessão (MaxSessionDuration, 1 hour). Só depois escolha a política a corrigir.

📝 **Como cai:** Política com condição que 'deveria funcionar' mas nega o uso legítimo.
Como resolver: Verifique se a chave de condição existe naquele contexto: aws:SourceIp via endpoint, aws:CalledVia em serviços que não a preenchem, chamadas feitas por principal de serviço (aws:PrincipalIsAWSService).

📝 **Como cai:** Acesso de muitas pessoas a muitas contas com o menor esforço.
Como resolver: IAM Identity Center com IdP externo (SAML + SCIM), permission sets por função, grupos e ABAC por atributos; JIT por acesso temporário elevado.

📝 **Como cai:** Perímetro de dados na organização.
Como resolver: Defina a direção: identidades internas indo para fora = SCP ou endpoint policy com aws:ResourceOrgID; externos entrando = RCP ou política de recurso com aws:PrincipalOrgID.

📝 **Como cai:** Delegar administração de IAM sem escalonamento.
Como resolver: Permitir CreateRole só com iam:PermissionsBoundary obrigatório, negar remover ou editar o boundary, usar IAM path para escopo.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
liberar recurso para toda a organização sem lista de contas	**aws:PrincipalOrgID**
terceiro acessando sua conta	**Role entre contas com ExternalId**
1 hour session limit com DurationSeconds alto	**Role chaining**
Encoded authorization failure message	**sts decode-authorization-message**
Response signature invalid após troca de certificado	**Atualizar metadados SAML no identity provider do IAM**
AROA... no Principal da trust policy	**Role recriada: salvar o ARN de novo**
servidor fora da AWS com certificado da PKI própria	**IAM Roles Anywhere**
GitHub Actions sem chave de acesso	**OIDC + AssumeRoleWithWebIdentity com condição no claim sub**

acesso temporário a objeto para quem não tem conta AWS	**URL pré-assinada**
JIT com aprovação para humanos	**Acesso temporário elevado sobre permission sets do Identity Center**
roles, chaves e permissões ociosas em toda a organização	**Analisador de acesso não utilizado do IAM Access Analyzer**
política mínima a partir do uso real	**Geração de política do Access Analyzer com o trail**
autorização por registro dentro da aplicação	**Amazon Verified Permissions com Cedar**
aws:RequestedRegion quebrando IAM, STS global ou CloudFront	**Deny + NotAction com os serviços globais**

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

- Deny explícito em qualquer camada vence qualquer Allow.
- SCP não concede permissão e não alcança service-linked roles nem a conta de gerenciamento.
- Role chaining limita a sessão a 1 hora.
- aws:SourceIp some quando a chamada passa por VPC endpoint.
- Mudou o permission set: reprovisione.

Essenciais para a prova (checklist)

- ☐ Sei avaliar uma requisição com identidade, boundary, session policy, SCP, RCP e política de recurso.
- ☐ Sei resolver erros de duração de sessão e role chaining.
- ☐ Sei escolher entre aws:PrincipalOrgID, aws:PrincipalOrgPaths, aws:ResourceOrgID e aws:SourceOrgID.
- ☐ Sei usar kms:ViaService, aws:CalledVia, aws:ViaAWSService e aws:PrincipalIsAWSService.
- ☐ Sei configurar ABAC com session tags e attributes for access control.
- ☐ Sei separar sessão do portal e session duration do permission set no Identity Center.
- ☐ Sei eliminar chaves de longo prazo com instance profile, Roles Anywhere, OIDC e Pod Identity.
- ☐ Sei usar os quatro tipos de análise do IAM Access Analyzer.
- ☐ Sei forçar MFA em usuários IAM e na CLI.
- ☐ Sei delegar criação de roles com permissions boundary sem escalonamento.

Questões de revisão do capítulo

R4.1 · Domínio 4: Gerenciamento de identidade e acesso

Uma empresa precisa dar acesso temporário a um provedor terceirizado, que tem conta AWS própria, para atividades de suporte em contas de produção. Os requisitos são: (1) nenhuma credencial de longa duração compartilhada; (2) identificar no CloudTrail as ações feitas pelo provedor; (3) revogar o acesso a qualquer momento; e (4) privilégio mínimo por função. Qual abordagem atende melhor a esses requisitos?

A. Role entre contas confiando na conta do provedor, com sts:ExternalId na trust policy e política de menor privilégio
B. Role entre contas confiando na conta do provedor, sem ExternalId, restrita pela condição aws:SourceIp aos IPs do provedor
C. Usuário do IAM Identity Center para cada técnico do provedor, com permission set de administrador nas contas
D. Usuário IAM com MFA para o provedor e chaves de acesso rotacionadas a cada 30 dias pelo Secrets Manager

R4.2 · Domínio 4: Gerenciamento de identidade e acesso

Uma operadora de saúde usa o IAM Identity Center com o Microsoft Entra ID como provedor de identidade. A política interna define que o usuário deve se autenticar de novo no portal de acesso da AWS a cada 4 horas, que as sessões do permission set AdminProducao nas contas devem durar no máximo 1 hora e que o permission set SomenteLeitura pode manter sessões de até 8 horas. Qual configuração atende a esses requisitos?

A. Editar no console do IAM de cada conta a duração máxima de sessão das roles AWSReservedSSO criadas para os dois permission sets, definindo 1 hora e 8 horas
B. Configurar 4 horas para os dois permission sets e 12 horas para a sessão interativa do portal, compensando a diferença com um alarme de sessões longas no CloudWatch
C. Configurar 4 horas como duração da sessão interativa do portal e definir a session duration de 1 hora no AdminProducao e de 8 horas no SomenteLeitura
D. Configurar 1 hora como duração da sessão interativa do portal, para que o fim da sessão do portal encerre também as sessões abertas nas contas AWS pelos dois permission sets

R4.3 · Domínio 4: Gerenciamento de identidade e acesso

Na conta A de uma rede de farmácias, um worker com a role Processador consome mensagens de uma fila SQS da conta B (criptografada com SSE-SQS) e grava o resultado em um bucket S3 da própria conta A, na mesma execução. O time quer evitar que o worker troque de credenciais entre a leitura da fila e a gravação no bucket, mantendo o menor privilégio. Qual configuração atende ao requisito?

A. Criar na conta A uma SCP que permita as ações sqs:ReceiveMessage e sqs:DeleteMessage no ARN da fila da conta B para a role Processador
B. Incluir na queue policy da fila da conta B as ações de leitura e exclusão de mensagens para a role Processador e as mesmas ações na política de identidade dessa role
C. Incluir na queue policy da fila da conta B as ações de leitura e exclusão de mensagens para a conta A, contando que o administrador de A não precise conceder mais nada
D. Criar na conta B uma role com permissão na fila e trust policy para a role Processador, e fazer o worker assumir essa role antes de ler cada lote de mensagens

R4.4 · Domínio 4: Gerenciamento de identidade e acesso

Uma plataforma de ensino a distância tem um aplicativo móvel que obtém credenciais temporárias por um identity pool do Amazon Cognito e acessa diretamente a tabela Anotacoes do DynamoDB, sem backend. A chave de partição da tabela é o identity ID do Cognito de cada aluno. A auditoria apontou que a role autenticada permite ler e gravar qualquer item da tabela. A equipe precisa garantir que cada aluno só leia e grave os próprios itens, sem criar uma role por aluno. Qual alteração na política da role autenticada atende a esse requisito?

A. Adicionar a condição StringEquals com aws:ResourceTag/Owner igual a ${cognito-identity.amazonaws.com:sub} e marcar cada item da tabela com a tag Owner contendo o identity ID do aluno
B. Adicionar a condição ForAllValues:StringEquals com a chave dynamodb:Attributes listando os atributos que cada aluno pode ler e atualizar na tabela
C. Criar um grupo no user pool para cada turma, mapear cada grupo para uma role IAM diferente e restringir cada role às partições da turma correspondente
D. Adicionar a condição ForAllValues:StringEquals com a chave dynamodb:LeadingKeys igual a ${cognito-identity.amazonaws.com:sub} nas ações de leitura e gravação da tabela

Respostas comentadas

R4.1. A) Role entre contas confiando na conta do provedor, com sts:ExternalId na trust policy e política de menor privilégio

Por quê: Para terceiros, a AWS recomenda uma role com trust policy para a conta do provedor exigindo sts:ExternalId, valor único combinado com o cliente que impede o confused deputy. O provedor recebe credenciais temporárias do AWS STS, as chamadas ficam no CloudTrail associadas à sessão da role e o acesso pode ser revogado alterando a trust policy ou revogando as sessões ativas.

✗ B) Incorreta. Sem ExternalId a role fica exposta ao problema do confused deputy, e restringir por IP não substitui essa proteção.

✗ C) Incorreta. Permissões de administrador violam o privilégio mínimo exigido.

✗ D) Incorreta. Mesmo com rotação, chaves de acesso de usuário IAM são credenciais de longa duração.

> **Dica de prova:** Terceiro acessando sua conta: role entre contas com ExternalId.

R4.2. C) Configurar 4 horas como duração da sessão interativa do portal e definir a session duration de 1 hora no AdminProducao e de 8 horas no SomenteLeitura

Por quê: O Identity Center tem dois controles separados. A sessão interativa do usuário (padrão de 8 horas, de 15 minutos a 90 dias) define quanto tempo ele fica autenticado no portal de acesso e nas aplicações gerenciadas. A session duration do permission set (padrão de 1 hora, máximo de 12) define quanto tempo dura a sessão de console ou CLI em cada conta. Mudanças valem para sessões novas.

✗ A) Incorreta. As roles AWSReservedSSO são gerenciadas pelo Identity Center e reprovisionadas a partir do permission set; a configuração deve ser feita no permission set.

✗ B) Incorreta. Não atende a nenhum dos limites pedidos: o portal duraria 12 horas e o AdminProducao 4 horas, e um alarme não encerra sessões.

✗ D) Incorreta. A sessão do portal e as sessões nas contas são independentes: a sessão em uma conta dura o que o permission set define, e 1 hora no portal ainda obrigaria todos a reautenticar mais do que o exigido.

> **Dica de prova:** Reautenticar no portal: duração da sessão do Identity Center. Tempo dentro da conta: session duration do permission set.

R4.3. B) Incluir na queue policy da fila da conta B as ações de leitura e exclusão de mensagens para a role Processador e as mesmas ações na política de identidade dessa role

Por quê: Serviços com políticas de recurso, como S3, SQS, SNS e KMS, permitem acesso entre contas sem AssumeRole: o principal mantém suas permissões e acessa o recurso compartilhado na mesma sessão, o que é útil para copiar dados entre contas. Ao assumir uma role, o principal troca suas permissões pelas da role enquanto usa a sessão. Em ambos os casos, o acesso entre contas exige Allow nos dois lados.

✗ A) Incorreta. SCPs não concedem permissões; elas só limitam o máximo que os principais da conta podem receber.

✗ C) Incorreta. Mesmo com a conta A como principal, a role Processador continua precisando de Allow na própria política de identidade; além disso, conceder à conta inteira é mais amplo que o necessário.

✗ D) Incorreta. Ao assumir a role da conta B, o worker abre mão das permissões da role Processador durante a sessão e precisaria alternar credenciais para gravar no bucket da conta A.

> **Dica de prova:** Ler na conta B e gravar na conta A com a mesma credencial: política de recurso (queue, bucket, topic, key policy), não AssumeRole.

R4.4. D) Adicionar a condição ForAllValues:StringEquals com a chave dynamodb:LeadingKeys igual a ${cognito-identity.amazonaws.com:sub} nas ações de leitura e gravação da tabela

Por quê: O DynamoDB oferece controle de acesso refinado com a chave de condição dynamodb:LeadingKeys, que avalia o valor da chave de partição dos itens acessados. Combinada com a variável ${cognito-identity.amazonaws.com:sub}, ela implementa isolamento por usuário em uma única role, padrão comum em aplicativos móveis sem backend.

✗ A) Incorreta. Tags se aplicam ao recurso tabela, não a itens individuais; aws:ResourceTag não diferencia os itens de cada aluno dentro da mesma tabela.

✗ B) Incorreta. dynamodb:Attributes restringe quais atributos (colunas) podem ser acessados, mas não impede o acesso aos itens de outros alunos.

✗ C) Incorreta. Uma role por turma ainda deixa cada aluno acessar os itens dos colegas da turma, e o mapeamento por grupo aumenta muito a administração sem atingir o isolamento por aluno.

Dica de prova: Cada usuário só vê os próprios itens do DynamoDB: dynamodb:LeadingKeys com a variável do usuário. dynamodb:Attributes limita colunas, não linhas.

05

CAPÍTULO 5 · 18% DA PROVA

Domínio 5: Proteção de dados

Aqui eu preciso dominar o AWS KMS de ponta a ponta (key policy, grants, contexto de criptografia, rotação, material importado, chaves multi-Região), as opções de criptografia do S3, imutabilidade com Object Lock e AWS Backup, segredos no Secrets Manager e criptografia em trânsito com ACM, Private CA, políticas TLS do ELB e parâmetros do RDS. A prova descreve um requisito de conformidade e oferece quatro opções que parecem criptografar; vence a que atende exatamente ao detalhe pedido: duas camadas, nem o root apaga, sem mudar código, chave de outra Região. Onde mais erro: achar que dá para ativar criptografia depois em EFS e RDS, confundir modo governance com compliance e esquecer que chaves gerenciadas pela AWS (aws/ebs, aws/dynamodb) não têm key policy editável nem servem para outra conta.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Chave gerenciada pelo cliente x chave gerenciada pela AWS

Só a chave do cliente tem key policy editável, rotação configurável e pode ser liberada a outra conta. A aws/ebs não pode ser usada por outra conta, então snapshots e AMIs criptografados com ela não são compartilháveis. Para copiar snapshot em outra conta, a key policy libera kms:DescribeKey, kms:CreateGrant, kms:Decrypt, kms:ReEncrypt* e kms:GenerateDataKey*.

Rotação automática do KMS

Vale para chaves simétricas gerenciadas pelo cliente com material gerado pelo KMS; período configurável, padrão 365 dias. A chave mantém ID, ARN e políticas, cifra dados novos com a versão mais recente e decifra os antigos com as anteriores, sem recriptografar. Chaves HMAC não têm rotação automática.

Material de chave importado (origem EXTERNAL)

Não tem rotação automática, apenas rotação sob demanda (NEW_KEY_MATERIAL + RotateKeyOnDemand), mantendo o ARN. O cliente prova a entropia, guarda a cópia original e responde pela durabilidade; pode definir expiração e usar DeleteImportedKeyMaterial para bloquear na hora, reimportando a mesma cópia para reativar. Não se importa material em chave criada com origem AWS_KMS nem em custom key store.

Exclusão de chave KMS

Agendar a exclusão impõe espera de 7 a 30 dias (padrão 30) e ao final é permanente. Prática segura: desabilitar antes, observar falhas no CloudTrail, agendar com espera longa e criar alarme para o erro 'is pending deletion'.

Contexto de criptografia

Pares chave-valor não secretos usados como AAD: o mesmo contexto é exigido para decifrar e aparece em texto claro no CloudTrail, servindo para auditoria. kms:EncryptionContext:chave e kms:EncryptionContextKeys permitem ou negam conforme o contexto; nunca coloque PII nele.

Condições de key policy

kms:ViaService restringe o uso a chamadas feitas por um serviço (ex.: dynamodb.REGIAO.amazonaws.com); com kms:EncryptionContext:aws:s3:arn limita a um bucket ou prefixo. aws:PrincipalTag isola chaves por ambiente. Separação de funções exige que administradores não tenham kms:PutKeyPolicy sem controle.

Grants do KMS

Permissão temporária e programática para usar uma chave em operações específicas, com restrição de contexto de criptografia, criada e removida sem alterar a key policy; RetireGrant ou RevokeGrant encerram o acesso ao fim. Na cópia de snapshot criptografado em outra conta, a key policy precisa liberar kms:CreateGrant à conta de destino.

Opções de criptografia no lado do servidor do S3

SSE-S3 é o padrão, com chaves do S3. SSE-KMS aplica uma camada com chave do KMS e auditoria. DSSE-KMS aplica duas camadas independentes com chaves do KMS (cabeçalho aws:kms:dsse). SSE-C exige a chave em cada requisição, fora do KMS. Exigir HTTPS: Deny + Bool aws:SecureTransport false.

S3 Bucket Key

Gera uma chave de nível de bucket derivada da chave KMS e reduz em até 99% as requisições ao KMS, mantendo a chave do cliente. DSSE-KMS não usa Bucket Key. Com Bucket Key ativo, os eventos do KMS no CloudTrail mostram o ARN do bucket em vez do ARN do objeto.

S3 Object Lock

WORM por versão de objeto; exige versionamento. Compliance: ninguém, nem o root, encurta ou remove a retenção. Governance: contornável com s3:BypassGovernanceRetention. Lifecycle pode mudar a classe e criar delete marker, mas não apaga versão bloqueada; Object Lock não protege a chave KMS.

Imutabilidade no AWS Backup

Vault Lock em modo compliance protege pontos de recuperação; governance pode ser desfeito. Logically air-gapped vault tem Vault Lock compliance e chave própria e é compartilhado por AWS RAM só com IDs de contas individuais, que restauram direto sem copiar. Retenção longa, cópia entre contas e sobreviver à exclusão do recurso: AWS Backup.

Criptografia definida só na criação

EFS: criar novo sistema criptografado e migrar com DataSync; em trânsito, mount helper com tls e política negando aws:SecureTransport false. RDS: snapshot, cópia criptografada com a chave do cliente e restauração; não dá para ativar na instância nem criar réplica criptografada dela. Snapshots antigos do EBS também precisam ser copiados com criptografia.

Criptografia por padrão do EBS

Faz cada volume novo ser criptografado com a chave padrão escolhida, que pode ser do cliente. É configuração por conta e por Região e não altera recursos antigos. Em várias contas: SCP com ec2:Encrypted para prevenir e remediação do Config para legados.

Chaves regionais e multi-Região

Chave KMS de uma Região não é usada em outra: cópia entre Regiões (DLM, AWS Backup, CRR do S3) usa chave da Região de destino. Chave multi-Região permite decifrar em outra Região sem chamar a origem e sem recriptografar, mas replicar só a chave não replica o segredo nem os dados.

Secrets Manager x Parameter Store

Secrets Manager tem rotação nativa e replicação entre Regiões (réplica acompanha a rotação, usa chave da Região de destino e pode ser promovida). Parameter Store é configuração simples e barata, sem rotação nativa; parâmetro String fica em texto claro. Em Lambda, use a Parameters and Secrets Lambda Extension ou cache com TTL; variável de ambiente, mesmo criptografada, não é cofre.

ACM e AWS Private CA

O ACM renova automaticamente os certificados que emite; com validação por DNS não exige ação enquanto o CNAME estiver publicado. Certificado importado não é renovado pelo ACM. Nomes internos e mTLS pedem AWS Private CA (hierarquia raiz e subordinada, compartilhada por RAM, modo de vida curta).

TLS no ELB e no RDS

A política de segurança do listener define protocolos e cifras: o console usa ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, mas CLI, CloudFormation e CDK usam ELBSecurityPolicy-2016-08, que aceita versões antigas. No RDS, TLS obrigatório vem de parameter group personalizado: require_secure_transport (MySQL, MariaDB) ou rds.force_ssl (PostgreSQL, SQL Server).

KMS, CloudHSM, custom key store e XKS

PKCS#11, JCE ou exportar chave: CloudHSM. Integração nativa com serviços e API simples: KMS. HSM de locatário único com integração nativa: custom key store do CloudHSM. Chave fora da AWS integrada ao KMS: external key store (XKS). Dados em uso protegidos até de root: Nitro Enclaves com atestado na key policy.

Macetes para memorizar

Criptografia do S3

S3 padrão, KMS audita, DSSE dobra, C você carrega a chave.

Object Lock

Compliance é cofre de banco; governance é cofre com chave reserva.

Rotação

Gerado pelo KMS gira sozinho; importado gira na mão.

Chaves da AWS

aws/qualquer-coisa não sai da conta e não muda de política.

Criação

EFS e RDS: nasceu sem criptografia, só renasce criptografado (novo + migração ou snapshot copiado).

Contexto de criptografia

Contexto é etiqueta pública: identifica, nunca esconde.

ACM

Emitido pelo ACM renova; importado é problema seu.

Tabela de memorização: não confunda

Quando é...	...e quando é
SSE-KMS Uma camada auditável, com opção de S3 Bucket Key para reduzir custo.	**DSSE-KMS** Exigência de duas camadas independentes de criptografia no servidor com chaves do KMS.
Object Lock modo compliance Nem o root nem administradores podem apagar ou encurtar a retenção.	**Object Lock modo governance** Proteção que usuários com s3:BypassGovernanceRetention podem contornar.

S3 Object Lock Retenção com prazo fixo, WORM, compatível com Lifecycle.	**MFA Delete** Proteger exclusão de versão e mudança de versionamento; root, só por CLI/API, sem Lifecycle.
Material gerado pelo KMS Rotação automática e zero gestão de durabilidade.	**Material importado** Prova de entropia própria, cópia fora da AWS, expiração e kill switch reversível.
Secrets Manager Rotação nativa e replicação entre Regiões.	**Parameter Store** Configuração simples e barata sem rotação.
Certificado emitido pelo ACM Renovação gerenciada automática.	**Certificado importado no ACM** Renovação e reimportação por conta do cliente; ACM só avisa a expiração.
AWS KMS Integração nativa com S3, RDS, EBS e auditoria no CloudTrail.	**AWS CloudHSM** PKCS#11, JCE, exportar chave ou HSM dedicado.

Números que caem

Item	Valor
Período padrão de rotação automática do KMS	**365 dias (configurável)**
Espera da exclusão agendada de chave KMS	**7 a 30 dias, padrão 30**
Redução de requisições ao KMS com S3 Bucket Key	**até 99%**
S3 Glacier Deep Archive	**retenção mínima cobrada de 180 dias e recuperação em até 48 horas**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Ativar criptografia em repouso no EFS existente com update-file-system.
Como não cair: Só se define na criação; crie um EFS criptografado e migre com DataSync.

⚠ **Alerta de prova:** Usar SSE-KMS com Bucket Key para atender a exigência de duas camadas.
Como não cair: Bucket Key reduz chamadas, não adiciona camada; duas camadas é DSSE-KMS.

⚠ **Alerta de prova:** Escolher Object Lock governance para 'ninguém consegue apagar'.
Como não cair: Governance é contornável com s3:BypassGovernanceRetention; use compliance.

⚠ **Alerta de prova:** Usar MFA Delete como retenção regulatória.
Como não cair: O dono com o MFA ainda apaga, e não aceita Lifecycle; retenção com prazo é Object Lock.

⚠ **Alerta de prova:** Compartilhar snapshot criptografado com aws/ebs para outra conta.
Como não cair: A key policy da aws/ebs não pode ser alterada; use chave do cliente liberada à conta de destino.

⚠ **Alerta de prova:** Habilitar rotação automática anual em chave com material importado.
Como não cair: Material importado só aceita rotação sob demanda.

⚠ **Alerta de prova:** Recriptografar os dados à mão depois de ativar a rotação.
Como não cair: O KMS guarda as versões anteriores e decifra os dados antigos sozinho.

⚠ **Alerta de prova:** Usar na cópia entre Regiões a mesma chave KMS da Região de origem.
Como não cair: Chaves de uma Região não funcionam em outra; use chave da Região de destino ou multi-Região.

⚠ **Alerta de prova:** Colocar nome e CPF no contexto de criptografia para rastrear.
Como não cair: O contexto aparece em texto claro no CloudTrail; use um identificador não sensível, como tenant_id.

⚠ **Alerta de prova:** Editar o parameter group padrão do RDS para exigir TLS.
Como não cair: Parameter group padrão é imutável; crie um personalizado e associe.

⚠ **Alerta de prova:** Bloquear TLS 1.0 com regra do AWS WAF.
Como não cair: A negociação termina no listener antes do WAF; defina a SslPolicy do listener.

⚠ **Alerta de prova:** Usar ELBSecurityPolicy-TLS13-1-3-2021-06 quando há parceiros em TLS 1.2.
Como não cair: Ela aceita só TLS 1.3; para TLS 1.2 ou superior use TLS13-1-2-Res.

⚠ **Alerta de prova:** Emitir certificado público do ACM para nome interno ou Private CA para site público.
Como não cair: CA pública não valida nome interno; certificado privado não é confiável para navegadores.

⚠ **Alerta de prova:** Compartilhar logically air-gapped vault com uma OU inteira.
Como não cair: Aceita só IDs de contas individuais.

Como cai na prova

📝 **Como cai:** Requisito regulatório de retenção e imutabilidade com restrição de custo.
Como resolver: Compliance se 'ninguém' apaga; versionamento obrigatório; Lifecycle para a classe mais barata compatível com o tempo de recuperação; Backup Vault Lock para backups.

📝 **Como cai:** Controle de chave: quem usa, por qual serviço, em qual ambiente, com auditoria.
Como resolver: Chave gerenciada pelo cliente + key policy com kms:ViaService, aws:PrincipalTag e kms:EncryptionContext; descarte chaves gerenciadas pela AWS e soluções com chave local.

📝 **Como cai:** Recurso legado sem criptografia.
Como resolver: Lembre o que não se ativa depois (EFS, RDS, snapshot antigo) e escolha o caminho de recriação; para EBS novo, criptografia por padrão por Região; para S3 antigo, Batch Operations Copy.

📝 **Como cai:** Criptografia em trânsito exigida por auditoria.
Como resolver: Identifique o salto: ALB = SslPolicy; RDS = parameter group personalizado; S3 e EFS = aws:SecureTransport; SageMaker distribuído = inter-container traffic encryption; Direct Connect = MACsec.

📝 **Como cai:** Segredo em aplicação de alto volume ou multi-Região.
Como resolver: Secrets Manager com rotação, execution role restrita ao ARN, extensão ou cache com TTL, replicação para DR; segredo entre contas exige chave do cliente, nunca aws/secretsmanager.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
duas camadas independentes de criptografia no servidor	**DSSE-KMS (aws:kms:dsse)**
milhões de objetos e custo alto de requisições ao KMS	**S3 Bucket Key**
imutável, nem o root apaga, mais barato	**Object Lock compliance + Lifecycle para Glacier Deep Archive**
kill switch reversível sem período de espera	**Material importado + DeleteImportedKeyMaterial + reimportação**
decifrar em outra Região sem chamar a origem	**Chave KMS multi-Região**
segredo atualizado na Região de DR	**Replicação de segredo do Secrets Manager**
certificado expirou e o site caiu	**Certificado público emitido pelo ACM com validação DNS**

mTLS entre serviços com nomes internos	**AWS Private CA compartilhada por RAM**
administradores não podem ler dados com criptografia transparente	**Chave do cliente + key policy com kms:ViaService e separação de funções**
snapshots EBS por tag com cópia para outra Região, sem código	**Amazon Data Lifecycle Manager**
ransomware com administrador comprometido e restauração em outra conta	**Logically air-gapped vault compartilhado por RAM**
mascarar PII nos logs do CloudWatch	**Política de proteção de dados + logs:Unmask**
assinatura verificável por terceiros sem conta AWS	**Chave KMS assimétrica SIGN_VERIFY + GetPublicKey**
achar dados sensíveis no S3	**Amazon Macie**

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

- Chaves gerenciadas pela AWS não têm key policy editável nem podem ser usadas por outra conta.
- Material importado: sem rotação automática; rotação sob demanda e cópia original sob sua guarda.
- Object Lock compliance exige versionamento e nem o root encurta.
- Chave KMS é regional: cópia entre Regiões usa chave do destino ou multi-Região.
- Contexto de criptografia é texto claro no CloudTrail: nada de PII.

Essenciais para a prova (checklist)

- ☐ Sei escolher entre SSE-S3, SSE-KMS, DSSE-KMS e SSE-C e quando usar Bucket Key.
- ☐ Sei configurar Object Lock compliance com Lifecycle e diferenciar de governance e MFA Delete.
- ☐ Sei compartilhar snapshot ou AMI criptografado com outra conta.
- ☐ Sei as regras de rotação para material gerado pelo KMS e importado.
- ☐ Sei usar contexto de criptografia e kms:ViaService em key policies.
- ☐ Sei corrigir EFS e RDS criados sem criptografia.
- ☐ Sei replicar segredos e usá-los em Lambda com cache.
- ☐ Sei quando o ACM renova sozinho e quando usar Private CA.
- ☐ Sei exigir TLS em ALB, RDS, S3 e EFS.
- ☐ Sei montar backup imutável resistente a ransomware com AWS Backup.

Questões de revisão do capítulo

R5.1 · Domínio 5: Proteção de dados

Uma seguradora recebe diariamente documentos de sinistros no Amazon S3 e precisa guardá-los por 10 anos de forma imutável, sem que nenhum usuário, nem o usuário raiz, consiga apagá-los ou encurtar a retenção. Depois dos primeiros 30 dias, os documentos quase nunca são lidos e uma recuperação em até 48 horas é aceitável. O diretor financeiro pede o menor custo de armazenamento possível. Qual solução atende a esses requisitos?

A. Criar um vault do Amazon S3 Glacier com uma política de Vault Lock que negue exclusões por 10 anos e copiar os documentos do bucket para o vault de forma automática depois de 30 dias
B. Habilitar S3 Object Lock em modo governance com retenção de 10 anos e usar S3 Intelligent-Tiering com as camadas opcionais de arquivamento ativadas no bucket
C. Habilitar versionamento com MFA Delete no bucket e uma regra de S3 Lifecycle que mova os objetos para S3 Standard-IA após 30 dias para reduzir custo
D. Habilitar S3 Object Lock no bucket com retenção padrão em modo compliance de 10 anos e uma regra de S3 Lifecycle que mova os objetos para S3 Glacier Deep Archive após 30 dias

R5.2 · Domínio 5: Proteção de dados

Uma seguradora precisa proteger os volumes EBS de suas instâncias EC2 e copiar diariamente os snapshots desses volumes para uma conta de backup separada na mesma organização. Os dados devem continuar criptografados nas cópias, o controle das chaves deve ficar centralizado na equipe de segurança, com rotação automática e trilha de auditoria de cada uso. Qual solução atende melhor a esses requisitos?

A. Usar uma chave simétrica gerenciada pelo cliente, com rotação automática e key policy que concede kms:CreateGrant e kms:Decrypt à conta de backup
B. Usar uma chave assimétrica RSA do KMS nos volumes e snapshots e entregar a chave pública à conta de backup para descriptografar as cópias
C. Usar a chave aws/ebs nos volumes e compartilhar os snapshots com a conta de backup para que ela faça as cópias com a própria chave
D. Usar uma chave com material importado e rotação automática anual, com um grant permanente que libera o uso da chave à conta de backup

R5.3 · Domínio 5: Proteção de dados

Uma organização precisa garantir que os backups de bancos de dados armazenados em um bucket Amazon S3 estejam criptografados com chaves do KMS gerenciadas pelo cliente, específicas de cada ambiente (desenvolvimento, homologação e produção). Os times não devem conseguir usar por engano a chave de outro ambiente ao executar os backups automatizados. Qual solução atende melhor a esse requisito com o menor esforço operacional?

A. Habilitar a criptografia padrão do bucket com SSE-S3 e usar SCPs do AWS Organizations para bloquear cada acesso não autorizado
B. Usar uma chave gerenciada pelo cliente por ambiente, com key policy condicionada a aws:PrincipalTag e ao contexto de criptografia do ambiente
C. Criar uma única chave gerenciada pelo cliente e usar condições na bucket policy do S3 para restringir o acesso por tags de recursos
D. Criar uma chave do cliente por conta AWS e permitir que os ambientes compartilhem a mesma chave, controlando os acessos só por políticas do IAM

R5.4 · Domínio 5: Proteção de dados

Um hospital consome um SaaS de laudos por imagem hospedado na conta AWS do fornecedor, atrás de um Network Load Balancer, e hoje acessa o serviço pela internet. A nova exigência é que o tráfego nunca passe pela internet, que só o hospital possa iniciar conexões e que o fornecedor não tenha nenhuma rota para a rede do hospital. As duas VPCs usam o mesmo bloco 10.0.0.0/16. Qual solução atende a esses requisitos?

A. Criar uma conexão de VPC peering entre a VPC do hospital e a do fornecedor, com security groups que liberem só a porta do serviço a partir das sub-redes de aplicação do hospital
B. Compartilhar pelo AWS RAM um transit gateway do hospital com a conta do fornecedor e criar tabelas de rotas que permitam só o tráfego entre as sub-redes envolvidas
C. Pedir ao fornecedor um endpoint service do AWS PrivateLink com o NLB, liberando a conta do hospital, e criar no hospital um interface VPC endpoint nas sub-redes de aplicação
D. Manter o acesso pela internet com um NAT gateway e TLS 1.3, pedindo ao fornecedor uma lista de permissões com os IPs elásticos do NAT gateway do hospital

Respostas comentadas

R5.1. D) Habilitar S3 Object Lock no bucket com retenção padrão em modo compliance de 10 anos e uma regra de S3 Lifecycle que mova os objetos para S3 Glacier Deep Archive após 30 dias

Por quê: O S3 Object Lock aplica WORM por versão de objeto: em modo compliance ninguém, nem o usuário raiz, encurta ou remove a retenção. Objetos bloqueados podem mudar de classe de armazenamento por S3 Lifecycle sem perder a proteção, o que permite combinar imutabilidade com o custo do S3 Glacier Deep Archive (retenção mínima cobrada de 180 dias e recuperação em até 48 horas).

✗ A) Incorreta. Vaults do S3 Glacier (Glacier Direct) estão em manutenção e fechados a novos clientes; o WORM recomendado para dados no S3 é o S3 Object Lock.

✗ B) Incorreta. No modo governance, usuários com s3:BypassGovernanceRetention conseguem remover a proteção, o que não atende à exigência de que ninguém consiga apagar.

✗ C) Incorreta. MFA Delete não impede que o dono do bucket com o dispositivo MFA apague versões, não aceita regras de Lifecycle e o Standard-IA custa bem mais que o Deep Archive.

> **Dica de prova:** Imutável, raro acesso e mais barato: Object Lock compliance + Lifecycle para Glacier Deep Archive.

R5.2. A) Usar uma chave simétrica gerenciada pelo cliente, com rotação automática e key policy que concede kms:CreateGrant e kms:Decrypt à conta de backup

Por quê: Para copiar um snapshot criptografado em outra conta, a conta de destino precisa usar a chave de origem: a key policy da chave gerenciada pelo cliente deve conceder a ela kms:DescribeKey, kms:CreateGrant, kms:Decrypt, kms:ReEncrypt* e kms:GenerateDataKey*. A chave aws/ebs tem key policy fixa e não pode ser usada por outra conta. Chaves gerenciadas pelo cliente com material gerado pelo KMS aceitam rotação automática, e cada uso fica no CloudTrail.

✗ B) Incorreta. O EBS só usa chaves simétricas do KMS, e uma chave pública não descriptografa dados.

✗ C) Incorreta. A key policy da chave aws/ebs não pode ser alterada para outra conta, então snapshots criptografados com ela não podem ser compartilhados nem copiados por outra conta.

✗ D) Incorreta. A rotação automática do KMS não está disponível para chaves com material importado; nelas a rotação é sob demanda, com importação de novo material.

> **Dica de prova:** Snapshot criptografado para outra conta: chave gerenciada pelo cliente com key policy liberando a conta de destino; aws/ebs não serve.

R5.3. B) Usar uma chave gerenciada pelo cliente por ambiente, com key policy condicionada a aws:PrincipalTag e ao contexto de criptografia do ambiente

Por quê: Separar uma chave do KMS por ambiente garante isolamento criptográfico. Na key policy, condições com aws:PrincipalTag (por exemplo, environment=prod nas roles dos jobs de backup) e com chaves kms:EncryptionContext (no S3, o contexto inclui aws:s3:arn com o bucket ou prefixo do ambiente) fazem com que só os jobs daquele ambiente consigam usar a chave dele.

✗ A) Incorreta. O SSE-S3 usa chaves gerenciadas pelo S3, o que não atende ao requisito de chaves do KMS gerenciadas pelo cliente por ambiente.

✗ C) Incorreta. Com uma chave só, não há segregação criptográfica entre ambientes, e a bucket policy controla o acesso ao bucket, não qual chave é usada.

✗ D) Incorreta. Compartilhar a chave entre ambientes não isola os dados de cada um e não impede o uso da chave errada.

> **Dica de prova:** Isolar chaves por ambiente: uma chave por ambiente + key policy com aws:PrincipalTag e kms:EncryptionContext.

R5.4. C) Pedir ao fornecedor um endpoint service do AWS PrivateLink com o NLB, liberando a conta do hospital, e criar no hospital um interface VPC endpoint nas sub-redes de aplicação

Por quê: No AWS PrivateLink, o provedor publica um endpoint service na frente de um NLB e escolhe quais principais podem se conectar; o consumidor cria um interface VPC endpoint, que recebe IPs da própria VPC. O tráfego é unidirecional (consumidor para provedor), não atravessa a internet e não exige rotas entre as VPCs, então CIDRs sobrepostos não são problema.

✗ A) Incorreta. VPC peering não funciona com blocos CIDR sobrepostos e cria rotas nos dois sentidos entre as redes.

✗ B) Incorreta. O transit gateway também roteia entre redes inteiras e não resolve a sobreposição de CIDR, além de dar ao fornecedor um caminho para a rede do hospital.

✗ D) Incorreta. O tráfego continuaria passando pela internet, o que viola o requisito principal.

Dica de prova: Consumir SaaS de parceiro sem internet, com CIDR sobreposto e sem expor sua rede: PrivateLink (endpoint service + interface endpoint).

06

CAPÍTULO 6 · 14% DA PROVA

Domínio 6: Fundamentos de segurança e governança

Aqui eu preciso saber governar muitas contas: AWS Organizations (SCP, RCP, declarative policies, backup policies, tag policies, delegação), Control Tower, StackSets, AWS Config com agregadores e conformance packs, Firewall Manager, Security Hub CSPM, CloudFormation Guard e Hooks, Service Catalog e AWS Artifact. A prova pergunta muito se o controle é preventivo, proativo ou detectivo, e a resposta certa costuma ser o que impede antes de acontecer e cobre contas futuras sem trabalho manual. Onde mais erro: esquecer que a conta de gerenciamento fica fora de SCPs e RCPs, confundir AWS Artifact (conformidade da AWS) com Config e Security Hub CSPM (conformidade dos meus recursos) e escolher Audit Manager, que está fechado a novos clientes.

Neste capítulo
18 tópicos-chave · 13 pegadinhas · 6 macetes · 13 gatilhos · 4 questões comentadas

Tópicos-chave

SCP

Limita o que os principais das contas da organização podem fazer; não concede permissão e não afeta a conta de gerenciamento nem service-linked roles. Negação central com exceção por role: Deny com ArnNotLike em aws:PrincipalArn. Impede que contas membro desliguem controles ou saiam da organização, até pelo root. Restringir Regiões: aws:RequestedRegion com exceção para serviços globais.

RCP

Resource control policy limita o acesso aos recursos das contas da organização por principais de fora (perímetro de dados). Também não se aplica a recursos da conta de gerenciamento, por isso não se rodam cargas de trabalho nela.

Declarative policy do EC2

Impõe configuração durável de serviço em toda a organização, como AMIs permitidas, IMDSv2 e bloqueio de AMI ou snapshot público. Image Builder produz AMIs, mas não impede lançamentos com AMIs não aprovadas.

Outras políticas do Organizations

Backup policy impõe plano de backup em todas as contas, imutável para elas (Vault Lock protege, não agenda). Tag policies padronizam chaves e valores de tags. AI services opt-out policy na raiz, com @@none para travar, impede que a AWS use seu conteúdo de IA. Delegation policy permite gerenciar SCPs, RCPs e outras políticas fora da conta de gerenciamento.

Administrador delegado

Serviços de segurança da organização são geridos fora da conta de gerenciamento por uma conta de administrador delegado. Em serviços regionais, designe em cada Região usada.

Gerenciamento centralizado de root

Remove credenciais root das contas membro; com sts:AssumeRoot ainda é possível executar tarefas privilegiadas como desbloquear uma bucket policy. A conta de gerenciamento mantém o próprio root, que precisa de MFA redundante, sem chaves, e-mail de grupo e alerta de login.

AWS Control Tower

Landing zone + Account Factory + controles para governança multi-conta pronta. Muitas contas antigas numa OU: Register OU; conta isolada: enroll account. Drift de SCP gerenciada: re-register da OU ou atualização da landing zone; não edite as SCPs aws-guardrails pelo Organizations. Recursos e SCPs personalizados aplicados às contas novas via Git: CfCT.

Controles preventivo, proativo e detectivo

Preventivo (SCP) impede a ação. Proativo (CloudFormation Hook) barra o recurso não conforme antes de existir, mesmo fora do pipeline. Detectivo (regra do AWS Config) avalia depois que o recurso existe e pega mudanças feitas no console.

CloudFormation Guard, cfn-lint e Hooks

Template inválido: cfn-lint. Template válido mas fora das regras da empresa: CloudFormation Guard no pipeline (preventivo, só enxerga templates). Regra do Config personalizada sem Lambda: custom policy rule em Guard. Bloquear no próprio CloudFormation: Hooks.

Proteções de stack do CloudFormation e StackSets

Mudança fora do CloudFormation: drift detection. Exclusão da stack: termination protection. Recurso em update: stack policy. StackSets service-managed com auto-deploy dentro da organização; contas de fora, self-managed com AdministrationRole e ExecutionRole.

AWS Config multi-conta

Agregador de organização (Add my organization) dispensa autorização por conta e inclui contas novas; advanced query no agregador dá inventário e conformidade sob demanda. Conformance pack organizacional aplica as mesmas regras e remediações em toda a organização. Remediação intermitente: configure retries e segundos e diagnostique com describe-remediation-execution-status. Provar SSE-KMS com chave aprovada: s3-default-encryption-kms com kmsKeyArns.

AWS Firewall Manager

Padroniza WAF, security groups e DNS Firewall em várias contas a partir da conta administradora, com remediação automática para recursos novos. Política de auditoria de conteúdo acha regras abertas e SGs sem uso ou redundantes; política de DNS Firewall com first rule groups dá prioridade central.

Security Hub CSPM com configuração central

Conformidade contínua com padrões (PCI DSS, CIS, FSBP), pontuação e visão de várias contas e Regiões com agregação. Exceção a um controle em toda a organização: desabilitar o controle na política de configuração central; suprimir achado não para a avaliação e desabilitar o padrão inteiro elimina outros controles.

AWS Artifact

Fornece relatórios de auditoria da própria AWS e acordos como o BAA. Não atesta a configuração dos recursos do cliente, que é responsabilidade dele pelo modelo de responsabilidade compartilhada.

AWS RAM

Compartilha sub-redes (VPC sharing), Private CA central, prefix lists e outros recursos entre contas, evitando duplicar CAs ou VPCs. Peering exigiria uma VPC por conta e não é transitivo.

Service Catalog

Launch constraint permite lançar produto sem permissão nos serviços por trás; template constraint restringe parâmetros. O Service Catalog assume a role de lançamento na conta de quem provisiona.

Estrutura de OUs e AWS SRA

OUs por função e controles (Security, Infrastructure, Workloads, Sandbox), nunca pelo organograma ou por Região; SCPs se aplicam a OUs e contas, não a tags. AWS SRA é a arquitetura de referência de segurança para várias contas; maior isolamento entre tenants é conta separada em OU própria.

Break-glass e Well-Architected

Acesso de emergência independente do IdP, MFA físico em cofre, alerta em cada uso e teste periódico. Revisão estruturada de práticas com plano de melhoria e milestones: Well-Architected Tool, pilar de segurança. Trusted Advisor de todas as contas: organizational view na conta de gerenciamento.

Macetes para memorizar

Quatro verbos da governança
Prevenir com SCP, padronizar com StackSets, detectar com Config, centralizar com trail da organização.

Dentro x fora
SCP segura quem é de casa; RCP segura a visita.

Conformidade
Artifact = boletim da AWS; Config e Security Hub CSPM = boletim seu.

Tempo do controle
Guard e Hook antes, SCP na hora, Config depois.

Conta de gerenciamento
Fica fora das cercas: sem workload, com root blindado.

CloudFormation
Drift vê mudança; termination protection segura exclusão; stack policy segura update.

Tabela de memorização: não confunda

Quando é...	...e quando é
AWS Artifact Relatório de conformidade da própria AWS ou acordo (BAA).	**AWS Config / Security Hub CSPM** Conformidade dos seus recursos ao longo do tempo.
CloudFormation Guard no pipeline Prevenção sobre templates antes do deploy.	**Regra do AWS Config** Detecção sobre recursos já existentes, inclusive criados no console.
Register OU Muitas contas antigas de uma OU de uma vez.	**Enroll account** Uma conta isolada.
StackSets service-managed Dentro da organização, com auto-deploy em contas novas.	**StackSets self-managed** Contas fora da organização, com AdministrationRole e ExecutionRole.
Launch constraint Usuário lança produto sem permissão nos serviços por trás.	**Template constraint** Restringir os parâmetros aceitos.
Well-Architected Tool Revisão de práticas com riscos, plano de melhoria e milestones.	**Trusted Advisor** Verificações periódicas (como portas irrestritas em security groups), que só sinalizam, sem remediação; de todas as contas, pelo organizational view.

Números que caem

Item	Valor
Valor que trava a AI services opt-out policy	**@@none**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Aplicar SCP ou RCP para proteger a conta de gerenciamento.
Como não cair: Ela fica fora das duas; não coloque cargas de trabalho nela.

⚠ **Alerta de prova:** Usar regra do Config para impedir que uma conta saia da organização.
Como não cair: Config é detectivo e não desfaz a saída; use SCP com Deny.

⚠ **Alerta de prova:** Usar Backup Vault Lock para impor plano de backup nas contas.
Como não cair: Vault Lock protege pontos de recuperação, não agenda; use backup policy do Organizations.

⚠ **Alerta de prova:** Suprimir achados ou desabilitar o padrão inteiro para aprovar uma exceção.
Como não cair: Desabilite só o controle na política de configuração central.

⚠ **Alerta de prova:** Recomendar AWS Audit Manager para coletar evidências ou relatórios.
Como não cair: Está fechado a novos clientes; relatórios da AWS no Artifact, conformidade dos recursos no Config e Security Hub CSPM.

⚠ **Alerta de prova:** Usar o relatório do AWS Artifact para atestar a configuração das contas da empresa.
Como não cair: Artifact atesta a infraestrutura da AWS, não os seus recursos.

⚠ **Alerta de prova:** Editar as SCPs aws-guardrails pelo Organizations para corrigir drift.
Como não cair: Isso causa o drift; resolva com re-register da OU ou atualização da landing zone.

⚠ **Alerta de prova:** Contar com Guard no pipeline para pegar recursos criados no console.
Como não cair: Guard só enxerga templates; mudanças no console exigem Config.

⚠ **Alerta de prova:** Organizar OUs por Região ou por tags.
Como não cair: Agrupe por função e requisitos de controle; SCP se aplica a OUs e contas, não a tags.

⚠ **Alerta de prova:** Compartilhar AMI publicamente e restringir com SCP.
Como não cair: AMI pública vale para qualquer conta; use launch permission com ARN da OU e chave do cliente liberada à OU.

⚠ **Alerta de prova:** Usar tag policy do Organizations para impedir que um principal troque a tag de autorização do ABAC.
Como não cair: Tag policy só padroniza valores (trocar prod por dev continua válido); negue CreateTags e DeleteTags para a chave de autorização com aws:TagKeys.

⚠ **Alerta de prova:** Exigir que cada dono de conta provisione o produto padrão.
Como não cair: Não é automático; use StackSets com auto-deploy, CfCT ou Firewall Manager.

⚠ **Alerta de prova:** Usar a regra s3-bucket-server-side-encryption-enabled para provar SSE-KMS.
Como não cair: Todo bucket já tem SSE-S3 por padrão, então ela fica conforme sem SSE-KMS; use s3-default-encryption-kms com kmsKeyArns.

Como cai na prova

📝 **Como cai:** Impor um padrão em todas as contas, inclusive futuras, com menor esforço.
Como resolver: Prefira políticas do Organizations (SCP, RCP, declarative, backup, tag), StackSets service-managed com auto-deploy, conformance pack organizacional ou Firewall Manager. Descarte soluções conta por conta e automação própria.

📝 **Como cai:** Escolher entre controle preventivo, proativo e detectivo.
Como resolver: Leia o verbo: 'impedir' ou 'antes de existir' = SCP ou Hook; 'detectar' e 'corrigir depois' = Config com remediação.

📝 **Como cai:** Pedido de evidência de conformidade para auditor.
Como resolver: Sobre a AWS: Artifact. Sobre seus recursos: Config (conformance packs, agregador) e Security Hub CSPM. Trusted Advisor de todas as contas: organizational view. Não use Audit Manager.

📝 **Como cai:** Drift ou falha em Control Tower e remediação.
Como resolver: Corrija pelo próprio Control Tower (re-register, atualização da landing zone); remediação do Config com retries; nunca edite controles gerenciados por fora.

📝 **Como cai:** Proteger root e acesso de emergência.
Como resolver: Gerenciamento centralizado de root nas contas membro, AssumeRoot para tarefas privilegiadas, root da conta de gerenciamento com MFA redundante; break-glass independente do IdP com alerta e teste.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
impor AMIs permitidas e IMDSv2 na organização	**Declarative policy do EC2**
bloquear principais externos aos recursos da organização	**RCP**
conta membro sem senha root e precisa desbloquear bucket policy	**Gerenciamento centralizado de root + sts:AssumeRoot**
barrar recurso não conforme antes de existir, mesmo fora do pipeline	**CloudFormation Hooks (controle proativo)**
inventário multi-conta sob demanda	**Advanced query do Config no agregador**
agregador sem autorização por conta e com contas novas	**Organization aggregator (Add my organization)**
relatório de auditoria da AWS ou BAA	**AWS Artifact**
várias contas usando a mesma VPC controlada por um time	**VPC sharing via AWS RAM**
uma Private CA central para várias contas	**Compartilhar a CA via AWS RAM**
impedir que a AWS use conteúdo de IA na organização	**AI services opt-out policy na raiz com @@none**
padronizar chaves e valores de tags	**Tag policies**
gerenciar políticas do Organizations fora da conta de gerenciamento	**Delegation policy do Organizations**
Terraform na AWS com segurança	**Estado no S3 com KMS, versionamento e use_lockfile, um backend por ambiente, role por conta**

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

- A conta de gerenciamento fica fora de SCPs e RCPs.
- Artifact é conformidade da AWS; Config e Security Hub CSPM são conformidade dos seus recursos.
- Audit Manager e CloudTrail Lake estão fechados a novos clientes.
- Config é detectivo; Guard e Hooks são preventivos ou proativos.
- Drift de Control Tower se corrige pelo Control Tower.

Essenciais para a prova (checklist)

- ☐ Sei a diferença entre SCP, RCP, declarative policy, backup policy e tag policy.
- ☐ Sei configurar administrador delegado e delegation policy fora da conta de gerenciamento.
- ☐ Sei usar gerenciamento centralizado de root e sts:AssumeRoot.
- ☐ Sei registrar OUs e contas no Control Tower e corrigir drift.
- ☐ Sei classificar Guard, Hooks, SCP e Config como preventivo, proativo ou detectivo.
- ☐ Sei montar agregador de organização e conformance packs organizacionais.
- ☐ Sei padronizar WAF, security groups e DNS Firewall com Firewall Manager.
- ☐ Sei aplicar exceção a um controle no Security Hub CSPM sem desligar o padrão.
- ☐ Sei quando usar AWS Artifact e quando usar Config ou Security Hub CSPM.
- ☐ Sei compartilhar sub-redes, Private CA e prefix lists com AWS RAM.

Questões de revisão do capítulo

R6.1 · Domínio 6: Fundamentos de segurança e governança

Uma organização quer que a equipe de segurança gerencie o GuardDuty e o Security Hub de todas as contas a partir de uma conta de segurança dedicada, sem usar a conta de gerenciamento do Organizations no dia a dia. O que deve configurar?

A. Uma role de administrador em cada conta-membro
B. Serviços ativados só na conta de gerenciamento
C. Administrador delegado na conta de segurança
D. Usuários IAM da equipe em cada conta

R6.2 · Domínio 6: Fundamentos de segurança e governança

Uma rede de escolas tem 80 contas no AWS Organizations, e cada time cria os próprios planos do AWS Backup, com frequências e retenções diferentes. A diretoria de risco exige que todo recurso com a tag backup=diario, em todas as contas e também nas futuras, tenha backup diário retido por 35 dias e cópia para um vault em outra Região, sem que os times das contas membro consigam alterar esse plano. Qual solução atende a esses requisitos com o MENOR esforço operacional?

A. Configurar no vault central um AWS Backup Vault Lock em modo compliance com retenção mínima de 35 dias e compartilhar esse vault com as contas pelo AWS RAM
B. Habilitar as backup policies no AWS Organizations e anexar à raiz uma política com plano diário, retenção de 35 dias, cópia entre Regiões e seleção pela tag
C. Implantar com CloudFormation StackSets e implantação automática um plano do AWS Backup em cada conta, protegido por uma SCP que negue backup:UpdateBackupPlan
D. Criar uma regra organizacional do AWS Config que marque como não conforme o recurso com a tag backup=diario sem ponto de recuperação nas últimas 24 horas

R6.3 · Domínio 6: Fundamentos de segurança e governança

A área de conformidade de uma operadora de logística precisa responder toda semana aos auditores quais recursos estão NON_COMPLIANT nas regras do AWS Config, em quais contas e Regiões, agrupados por tipo de recurso. A organização já tem um agregador de organização na conta de auditoria. A equipe quer obter a lista sob demanda, sem exportar dados nem manter infraestrutura de consulta. Qual solução atende a esses requisitos?

A. Criar um dashboard do CloudWatch na conta de auditoria com as métricas de uso do AWS Config de cada conta e Região da organização
B. Executar em cada conta e Região o comando describe-compliance-by-resource e consolidar as saídas em uma planilha compartilhada com os auditores
C. Habilitar a entrega de snapshots de configuração do Config em cada conta para um bucket central e consultar os arquivos no Athena agrupando por tipo
D. Executar uma consulta avançada do AWS Config no agregador, filtrando AWS::Config::ResourceCompliance por complianceType NON_COMPLIANT

R6.4 · Domínio 6: Fundamentos de segurança e governança

A equipe de governança de uma rede de hospitais precisa avaliar continuamente uma regra interna: toda tabela do Amazon DynamoDB com a tag classificacao=restrita deve ter point-in-time recovery habilitado e criptografia com chave KMS gerenciada pelo cliente, com mensagem de não conformidade explicando o motivo. As tabelas são criadas por pipelines e também pelo console. A equipe não quer manter código nem runtime de funções para essa avaliação. Qual solução atende a esses requisitos com o MENOR esforço operacional?

A. Executar o CloudFormation Guard no pipeline com a regra interna e reprovar o deploy dos templates que criarem tabelas fora do padrão
B. Criar uma automation rule do Security Hub CSPM que marque como NOTIFIED os achados das tabelas com a tag classificacao=restrita
C. Criar uma regra personalizada do AWS Config apoiada em uma função Lambda que leia o item de configuração da tabela e devolva a avaliação com PutEvaluations
D. Criar uma regra personalizada do AWS Config do tipo custom policy, escrita em CloudFormation Guard, acionada por mudanças de configuração das tabelas

Respostas comentadas

R6.1. C) Administrador delegado na conta de segurança

Por quê: Serviços como GuardDuty, Security Hub, Macie e Inspector permitem designar uma conta-membro como administrador delegado da organização. Assim, a conta de segurança habilita e gerencia o serviço em todas as contas, e a conta de gerenciamento fica restrita a tarefas de governança, seguindo o princípio de menor privilégio.

✗ A) Incorreta. Descentraliza e amplia privilégios sem gestão unificada.
✗ B) Incorreta. Exige usar a conta de gerenciamento no dia a dia.
✗ D) Incorreta. Multiplica credenciais e não centraliza os serviços.

> **Dica de prova:** Gerir serviços de segurança da organização fora da conta de gerenciamento: administrador delegado.

R6.2. B) Habilitar as backup policies no AWS Organizations e anexar à raiz uma política com plano diário, retenção de 35 dias, cópia entre Regiões e seleção pela tag

Por quê: Backup policies do AWS Organizations combinam em JSON o plano de backup (frequência, janela, retenção, cópias), a seleção de recursos por tags e a role IAM usada pelo AWS Backup, e são herdadas pelas contas da raiz ou das OUs. Na conta membro, o plano efetivo pode ser visto mas não alterado. A role referenciada precisa existir em cada conta.

✗ A) Incorreta. O Vault Lock protege os pontos de recuperação contra exclusão antecipada, mas não cria backups nem define frequência, seleção por tag ou cópia entre Regiões.
✗ C) Incorreta. Pode funcionar, mas exige manter templates, StackSets e uma SCP para proteger o plano, quando as backup policies já entregam um plano imutável para as contas membro.
✗ D) Incorreta. É um controle detectivo: aponta a falta de backup, mas não cria nem impõe o plano.

> **Dica de prova:** Impor plano de backup em todas as contas, imutável para elas: backup policy do Organizations. Vault Lock protege, não agenda.

R6.3. D) Executar uma consulta avançada do AWS Config no agregador, filtrando AWS::Config::ResourceCompliance por complianceType NON_COMPLIANT

Por quê: AWS Config advanced query consulta, com sintaxe semelhante a SQL SELECT, o estado atual de recursos e dados de conformidade, como AWS::Config::ResourceCompliance e AWS::Config::ConformancePackCompliance. Executada em um agregador, a mesma consulta cobre todas as contas e Regiões agregadas, sem exportação.

✗ A) Incorreta. As métricas de uso do Config não listam os recursos não conformes por conta, Região e tipo.

✗ B) Incorreta. Exige percorrer cada conta e Região e consolidar resultados por fora, com muito trabalho a cada semana.

✗ C) Incorreta. Funciona, mas cria exportação, tabelas e consultas para manter, o que a equipe quer evitar.

> **Dica de prova:** Inventário ou conformidade multi-conta sob demanda: advanced query do Config no agregador.

R6.4. D) Criar uma regra personalizada do AWS Config do tipo custom policy, escrita em CloudFormation Guard, acionada por mudanças de configuração das tabelas

Por quê: O AWS Config oferece dois tipos de regra personalizada: apoiada em Lambda e custom policy, escrita em Guard. A custom policy roda a lógica dentro do próprio Config, sem função para manter, e na avaliação detetiva é acionada por mudanças de configuração (escopo por tipo de recurso, tag ou todas as mudanças). Também pode habilitar avaliação proativa antes do provisionamento.

✗ A) Incorreta. O Guard no pipeline é um controle preventivo que só enxerga templates; tabelas criadas pelo console e mudanças posteriores não seriam avaliadas.

✗ B) Incorreta. Automation rules alteram campos de achados existentes, como severidade e status de workflow; não avaliam configuração de recursos nem criam controles.

✗ C) Incorreta. Uma regra apoiada em Lambda funciona, mas exige manter código, runtime e permissões da função, o que a equipe quer evitar.

> **Dica de prova:** Regra do Config personalizada sem Lambda = custom policy rule em Guard. Guard no pipeline é preventivo; Config é detetivo e pega mudanças feitas no console.

DIA DA PROVA

Estratégia de prova

A SCS-C03 é uma prova de cenário: cada enunciado traz uma empresa, um incidente ou uma auditoria e várias restrições escondidas (sem código, sem internet, contas futuras, nem o root, sem mudar a aplicação, menor esforço operacional). Quase sempre duas alternativas 'funcionam', mas só uma cumpre todas as restrições; as erradas costumam ser detectivas quando se pede prevenção, manuais quando se pede automação ou destrutivas quando se pede preservar evidência. A prova valoriza o recurso gerenciado e nativo exato, com o detalhe técnico certo (chave de condição, modo de retenção, Região da chave, camada de rede). Mensagens de erro reais e fluxos de investigação aparecem com frequência, e a ordem dos passos conta tanto quanto o serviço.

Como responder

✓ São 65 questões em 170 minutos (50 pontuadas e 15 não pontuadas, sem identificação): reserve cerca de 2 minutos e meio por questão e marque as longas para revisão.

✓ A pontuação vai de 100 a 1000 com mínimo de 750 e é compensatória: não precisa passar em cada domínio, então não trave em um tema difícil.

✓ Questão em branco conta como errada e não há penalidade por chute: responda todas antes de revisar.

✓ Antes das alternativas, sublinhe as restrições do enunciado (sem código, sem internet, nem o root, contas futuras, menor esforço) e use cada uma para eliminar opções.

✓ Em múltipla resposta, a quantidade pedida vem no enunciado; escolha alternativas que se complementam, não duas que fazem a mesma coisa.

✓ Em ordenação e correspondência só há crédito com tudo certo: na ordem forense, metadados antes de mudar security group, role ou tags, memória antes do disco e nada de parar ou encerrar antes da coleta.

✓ Desconfie de alternativas com Lambda, script ou cron quando existe recurso nativo (remediação do Config, automation rules, DLM, replicação de segredo).

✓ Os pesos favorecem IAM (20%), infraestrutura (18%) e proteção de dados (18%): domine avaliação de políticas, KMS e rede antes de detalhes raros.

Erros que derrubam candidatos

✗ Escolher um controle detectivo (Config, alarme, EventBridge) quando o enunciado pede impedir ou prevenir.

✗ Achar que SCP concede permissão ou que alcança a conta de gerenciamento e service-linked roles.

✗ Destruir evidência: encerrar instância, apagar pod, função ou segredo antes de coletar.

✗ Esquecer o aspecto regional: chave KMS da Região errada, regra do EventBridge ou administrador delegado em outra Região.

✗ Confundir modos e variantes parecidas: Object Lock governance x compliance, SSE-KMS x DSSE-KMS, aws:CalledVia x aws:ViaAWSService.

✗ Usar chaves gerenciadas pela AWS em cenários que exigem compartilhamento entre contas ou key policy restritiva.

✗ Recomendar serviços fechados a novos clientes, como Audit Manager, CloudTrail Lake e vaults do S3 Glacier.

Na semana da prova

- ☐ Refaça as provas e revise só as alternativas erradas, anotando o detalhe que as derruba.
- ☐ Releia as seções Lembrar e Pegadinhas de cada domínio, priorizando IAM, proteção de dados e infraestrutura.
- ☐ Treine em voz alta a ordem forense e a ordem de rotação de access key, que aparecem como ordenação.
- ☐ Monte uma tabela de uma página com fontes de log x pergunta investigativa e SCP x RCP x política de recurso.
- ☐ Na véspera, nada de conteúdo novo: revise macetes e números, durma bem e confirme horário e documento.

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: Detecção

‣ qual domínio a instância consultou → **Route 53 Resolver query logs**

‣ ataque em vários estágios virando um único achado crítico → **GuardDuty Extended Threat Detection (AttackSequence)**

‣ arquivo enviado por usuário precisa ser varrido antes do uso → **GuardDuty Malware Protection for S3 + bucket policy pela tag do resultado**

‣ exfiltração anômala no S3 sem código e sem data events → **GuardDuty S3 Protection**

‣ InstanceCredentialExfiltration.OutsideAWS → **Credencial do instance profile usada fora da AWS: revogar sessões da role e exigir IMDSv2**

⚠ Flow Logs não mostram nomes nem capturam tráfego para o servidor DNS da Amazon; a fonte é Resolver query logs.

⚠ GetObject é evento de dados; sem data events habilitados, o download não aparece no trail.

⚠ Supressão arquiva o achado e o tira da fila dos analistas e das sequências do Extended Threat Detection; para reduzir alerta, filtre severidade na regra do EventBridge.

2. Domínio 2: Resposta a incidentes

‣ quem mais falou com este IP → **Perfil de entidade de IP no Amazon Detective**

‣ verificar malware em EC2 sem agente e sem achado do GuardDuty → **On-demand malware scan do GuardDuty pelo ARN da instância**

‣ sessão do atacante continua depois de trocar o SG → **Rastreamento de conexão; Deny na NACL**

‣ parar uma Lambda sem destruir evidência → **Concorrência reservada 0**

‣ aprovação de analista que pode levar horas → **Step Functions Standard com .waitForTaskToken ou aws:approve no SSM Automation**

⚠ Isso afeta só novas chamadas AssumeRole; sessões emitidas seguem válidas. Revogue com aws:TokenIssueTime.

⚠ Perde memória volátil e pode apagar volumes; colete memória e snapshot primeiro.

⚠ Nenhum dos dois impede a substituição por health check; desanexe ou coloque em Standby.

3. Domínio 3: Segurança de infraestrutura

‣ camada 2 no Direct Connect sem perder vazão → **MACsec em conexão dedicada**

‣ CIDR sobreposto, sem peering, só o cliente inicia → **PrivateLink (endpoint service + NLB + interface endpoint)**

‣ SSRF contra 169.254.169.254 → **IMDSv2 obrigatório, hop limit 1, na launch template**

‣ sem portas abertas, sem chaves SSH, sessões registradas → **Session Manager**

‣ controle L7 entre serviços de várias VPCs sem appliances → **VPC Lattice**

⚠ WAF se associa a CloudFront, ALB, API Gateway, AppSync e similares; nunca NLB nem TGW.

⚠ NACL é stateless: libere a saída para portas efêmeras 1024-65535; SG já deixa o retorno passar.

⚠ O tráfego para 169.254.169.254 não passa por eles; exija IMDSv2 com hop limit 1.

4. Domínio 4: Gerenciamento de identidade e acesso

‣ liberar recurso para toda a organização sem lista de contas → **aws:PrincipalOrgID**

‣ terceiro acessando sua conta → **Role entre contas com ExternalId**

‣ 1 hour session limit com DurationSeconds alto → **Role chaining**

‣ Encoded authorization failure message → **sts decode-authorization-message**

‣ Response signature invalid após troca de certificado → **Atualizar metadados SAML no identity provider do IAM**

⚠ SCP não concede permissão; sem Allow na política de identidade continua negado.

⚠ É role chaining, limitado a 1 hora independentemente da configuração; renove a sessão.

⚠ A chave some do contexto via endpoint; use aws:SourceVpce no mesmo Deny.

5. Domínio 5: Proteção de dados

‣ duas camadas independentes de criptografia no servidor → **DSSE-KMS (aws:kms:dsse)**

‣ milhões de objetos e custo alto de requisições ao KMS → **S3 Bucket Key**

‣ imutável, nem o root apaga, mais barato → **Object Lock compliance + Lifecycle para Glacier Deep Archive**

‣ kill switch reversível sem período de espera → **Material importado + DeleteImportedKeyMaterial + reimportação**

‣ decifrar em outra Região sem chamar a origem → **Chave KMS multi-Região**

⚠ Só se define na criação; crie um EFS criptografado e migre com DataSync.

⚠ Bucket Key reduz chamadas, não adiciona camada; duas camadas é DSSE-KMS.

⚠ Governance é contornável com s3:BypassGovernanceRetention; use compliance.

6. Domínio 6: Fundamentos de segurança e governança

‣ impor AMIs permitidas e IMDSv2 na organização → **Declarative policy do EC2**

‣ bloquear principais externos aos recursos da organização → **RCP**

‣ conta membro sem senha root e precisa desbloquear bucket policy → **Gerenciamento centralizado de root + sts:AssumeRoot**

‣ barrar recurso não conforme antes de existir, mesmo fora do pipeline → **CloudFormation Hooks (controle proativo)**

‣ inventário multi-conta sob demanda → **Advanced query do Config no agregador**

⚠ Ela fica fora das duas; não coloque cargas de trabalho nela.

⚠ Config é detectivo e não desfaz a saída; use SCP com Deny.

⚠ Vault Lock protege pontos de recuperação, não agenda; use backup policy do Organizations.

GABARITO

Respostas do diagnóstico

D1. D) Configurar o Route 53 Resolver query logging na VPC, enviando os registros para o CloudWatch Logs ou para o S3 com os nomes consultados e o ID da instância → revise o capítulo 1

Por quê: VPC Flow Logs não registram o tráfego para o servidor DNS da Amazon, para o serviço de metadados (169.254.169.254), para o Amazon Time Sync nem DHCP. Para ver consultas DNS, use o Route 53 Resolver query logging, que entrega em CloudWatch Logs, S3 ou Data Firehose.

✗ A) Incorreta. Os Flow Logs não capturam o tráfego para o servidor DNS da Amazon em nenhum formato, além de não mostrarem os nomes consultados.

✗ B) Incorreta. O CloudTrail registra chamadas à API do Route 53, como alterações de zonas, não as consultas DNS feitas ao resolvedor.

✗ C) Incorreta. O GuardDuty consome os logs de DNS como fonte própria de detecção, mas não os disponibiliza para exportação.

> **Dica de prova:** Flow Logs não mostram DNS da Amazon nem IMDS. Domínios consultados: Resolver query logs.

D2. D) Recriar o stream do Data Firehose com nome iniciado por aws-waf-logs-, por exemplo aws-waf-logs-producao, e selecioná-lo na configuração de logging → revise o capítulo 1

Por quê: Os destinos de log do AWS WAF precisam ter nomes iniciados por aws-waf-logs-. Para o Firehose, o stream deve ser Direct PUT e estar na Região do web ACL (us-east-1 para CloudFront).

✗ A) Incorreta. us-east-1 é exigido para web ACLs do CloudFront; para um web ACL regional, o stream fica na mesma Região do web ACL.

✗ B) Incorreta. Requisições amostradas e métricas são recursos independentes; não são pré-requisito para o logging nem fazem o stream aparecer.

✗ C) Incorreta. Essa política é necessária para entrega direta em bucket do S3; o destino aqui é o Data Firehose, que já tem permissões testadas.

> **Dica de prova:** Logs do WAF não aparecem: confira o prefixo aws-waf-logs- no nome do destino.

D3. A) Configurar no trail eventos de dados do S3 com seletor avançado em resources.ARN começando pelo prefixo e ativar a validação de integridade dos arquivos de log → revise o capítulo 1

Por quê: Para auditoria por identidade IAM no nível do objeto, o CloudTrail com eventos de dados do S3 é a escolha: registra o userIdentity, entrega em cerca de 5 minutos, permite seletores avançados por prefixo e oferece validação de integridade. Os logs de acesso do servidor cobrem casos como falhas de autenticação e transições de lifecycle, mas são de melhor esforço e sem digest.

✗ B) Incorreta. O S3 Inventory lista objetos e metadados, mas não registra requisições nem a identidade de quem leu ou apagou um objeto.

✗ C) Incorreta. GetObject e DeleteObject são eventos de dados; eventos de gerenciamento registram operações de bucket (como PutBucketPolicy), não leituras de objetos.

✗ D) Incorreta. Os logs de acesso do servidor são entregues em regime de melhor esforço, em algumas horas, não filtram por prefixo e não têm validação de integridade por assinatura digital.

> **Dica de prova:** Identidade IAM + integridade + prefixo = eventos de dados do CloudTrail. Falha de autenticação e lifecycle = logs de acesso do servidor.

D4. A) Executar uma restauração para um ponto no tempo às 14h00 em uma instância nova, isolar a instância comprometida por security group e tirar um snapshot dela, e apontar a aplicação para a nova → revise o capítulo 2

Por quê: A restauração para um ponto no tempo do RDS usa backups automáticos e logs de transação para criar uma nova instância em qualquer momento dentro do período de retenção. Como a instância original não é alterada, ela pode ser isolada e preservada como evidência, separando recuperação e investigação.

✗ B) Incorreta. Restaurar o snapshot da madrugada perde as transações legítimas até 14h00, e excluir a instância descarta a evidência original.

✗ C) Incorreta. O RDS não restaura um snapshot sobre uma instância existente; toda restauração cria uma instância nova. Além disso, sobrescrever a instância destruiria a evidência.

✗ D) Incorreta. Backtrack é um recurso do Aurora MySQL, não do RDS for PostgreSQL, e retrocede a própria instância, alterando o estado que o jurídico quer preservar.

> **Dica de prova:** Recuperar RDS ao momento antes da adulteração e preservar evidência: point-in-time restore em instância nova; a original fica isolada para a perícia.

D5. A) Aplicar SCP que nega o uso da role comprometida, isolar as instâncias com security groups de quarentena sem saída, proteger os logs e coletar evidências pela conta de segurança → revise o capítulo 2

Por quê: A contenção deve mirar o principal comprometido: uma SCP com Deny condicionado a aws:PrincipalArn da role interrompe o uso dela em todas as contas da OU, e revogar as sessões ativas da role completa o bloqueio. Security groups de quarentena sem regras de saída cortam a exfiltração e preservam a memória das instâncias. Os logs ficam protegidos (CloudTrail ativo, bucket com Object Lock), e a coleta de evidências parte da conta de segurança.

✗ B) Incorreta. Mover contas de OU no meio do incidente traz risco, negar só leitura no S3 não contém a role e ativar o Config é medida de longo prazo, não de contenção.

✗ C) Incorreta. Shield e WAF não tratam credenciais comprometidas no plano de controle, e mover buckets durante o incidente altera as evidências e afeta as aplicações.

✗ D) Incorreta. Bloquear S3 e AssumeRole em todas as contas para a produção, pausar o CloudTrail elimina rastreabilidade e encerrar instâncias destrói a memória.

> **Dica de prova:** Role comprometida em várias contas: SCP negando a role, quarentena por security group, logs protegidos e coleta central de evidências.

D6. A) Abrir no Amazon Detective o perfil da entidade do endereço IP 198.51.100.77 e analisar os painéis de interação com recursos e de chamadas de API no período do incidente → revise o capítulo 2

Por quê: O Amazon Detective monta um behavior graph a partir de CloudTrail, VPC Flow Logs, findings do GuardDuty e outras fontes. O perfil de uma entidade, como um endereço IP, concentra a atividade dela no tempo, incluindo os recursos que interagiram com o IP, o que acelera a validação do escopo e a análise de causa raiz.

✗ B) Incorreta. O Network Access Analyzer mostra caminhos de rede possíveis pela configuração, não as comunicações que de fato aconteceram com o IP.

✗ C) Incorreta. As consultas no Athena trazem a mesma informação, mas exigem escrever e ajustar SQL em várias fontes, o que o líder quer evitar.

✗ D) Incorreta. A busca mostra só os recursos que geraram findings; recursos que trocaram tráfego com o IP sem disparar um finding ficariam fora do escopo.

> **Dica de prova:** Quem mais falou com este IP? Perfil de entidade de IP no Amazon Detective.

D7. C) SG do RDS aceitando o SG das instâncias autorizadas; SG do bastion com SSH/RDP do IP fixo da equipe; instâncias privadas aceitando SSH/RDP do SG do bastion → revise o capítulo 3

Por quê: Security groups são stateful e podem usar outro security group como origem, o que permite encadear camadas sem depender de CIDRs. O SG do RDS aceita apenas o SG das instâncias autorizadas, o SG das instâncias aceita SSH/RDP apenas do SG do bastion e o SG do bastion aceita apenas o IP fixo da equipe. NACLs são stateless e servem para filtros amplos de sub-rede, não para esse controle fino.

✗ A) Incorreta. Anexar o SG do bastion às instâncias privadas não restringe a origem ao bastion; a regra correta é referenciar o SG do bastion como origem no SG das instâncias.

✗ B) Incorreta. Abre SSH/RDP da internet direto para a sub-rede privada, violando o requisito de acesso só pelo bastion, e libera o banco para toda a sub-rede.

✗ D) Incorreta. Liberar o banco para a VPC inteira e o bastion para a internet amplia a superfície de ataque; IAM não filtra tráfego de rede.

> **Dica de prova:** Camadas bastion, aplicação e banco: security groups referenciando security groups.

D8. D) Habilitar MACsec na conexão dedicada, associar um par CKN/CAK com associate-mac-sec-key, configurar o mesmo par no roteador e usar o modo must_encrypt → revise o capítulo 3

Por quê: MACsec no Direct Connect é a resposta quando o requisito é criptografia de camada 2 no enlace entre o roteador do cliente e a AWS, em conexões dedicadas compatíveis (10, 100 ou 400 Gbps) ou LAGs. A chave é um par CKN/CAK estático, associado com associate-mac-sec-key, e o modo must_encrypt garante que nada trafegue sem criptografia. Conexões hospedadas não suportam MACsec.

✗ A) Incorreta. A VPN IPsec criptografa na camada 3, depende de túneis com vazão limitada por túnel e adiciona sobrecarga de encapsulamento, o que não atende à exigência de camada 2 sem reduzir a vazão.

✗ B) Incorreta. MACsec não é suportado em conexões hospedadas; ele opera entre dois dispositivos específicos em conexões dedicadas e LAGs.

✗ C) Incorreta. TLS protege cada aplicação na camada de transporte e depende de cada serviço, que é justamente o que a auditoria quer evitar; o enlace físico continuaria sem criptografia de camada 2.

> **Dica de prova:** Direct Connect + camada 2 + sem perder vazão = MACsec em conexão dedicada. Criptografia em camada 3 sobre DX = Site-to-Site VPN.

D9. B) Endpoints de interface para ssm, ssmmessages e ec2messages, com HTTPS liberado no security group → revise o capítulo 3

Por quê: Sem acesso à internet, o SSM Agent depende de endpoints de interface para com.amazonaws.região.ssm e com.amazonaws.região.ssmmessages, que transporta o canal de dados do Session Manager; a documentação também lista ec2messages, embora versões recentes do agente prefiram ssmmessages quando disponível. O security group dos endpoints precisa aceitar HTTPS (443) das sub-redes das instâncias.

✗ A) Incorreta. Sem o endpoint ssmmessages, o canal de dados seguro usado pelo Session Manager não é estabelecido e as sessões falham.

✗ C) Incorreta. O NAT gateway funciona, mas leva o tráfego até os endpoints públicos do serviço pela internet, o que contraria o requisito.

✗ D) Incorreta. O gateway endpoint do S3 atende só ao Amazon S3 (por exemplo, atualização do agente); não substitui os endpoints do Systems Manager.

> **Dica de prova:** Session Manager sem internet: endpoints de interface ssm, ssmmessages e ec2messages.

D10. C) Permitir à role dos DBAs as ações de criptografia da chave com a condição kms:ViaService igual a rds.sa-east-1.amazonaws.com → revise o capítulo 4

Por quê: A condição kms:ViaService permite ou nega o uso de uma chave KMS conforme o serviço da AWS que faz a requisição em nome do principal (forward access session), por exemplo rds.sa-east-1.amazonaws.com ou ec2.sa-east-1.amazonaws.com. Para funcionar como restrição, não pode haver outra permissão da role (na key policy ou em política IAM) que libere a chave sem essa condição.

✗ A) Incorreta. aws:CalledVia só é preenchida por alguns serviços que fazem chamadas encadeadas com as credenciais do principal, e o RDS não está entre eles; a condição não restringe o uso da chave ao RDS.

✗ B) Incorreta. Restringe a conta de origem da chamada, mas uma chamada direta pelo CLI na mesma conta continuaria permitida.

✗ D) Incorreta. As chamadas que o RDS faz ao KMS em nome do usuário partem do próprio serviço, não de um VPC endpoint da sua VPC, então a condição negaria o uso legítimo.

> **Dica de prova:** Chave usável só através de um serviço: kms:ViaService com serviço.Região.amazonaws.com.

D11. A) Trocar o Principal da trust policy da role de ec2.amazonaws.com para lambda.amazonaws.com com a ação sts:AssumeRole → revise o capítulo 4

Por quê: Toda role de serviço tem duas partes: a trust policy, que diz quem pode assumir a role (para Lambda, o service principal lambda.amazonaws.com), e as políticas de permissão, que dizem o que a role pode fazer. iam:PassRole é a permissão de quem configura o serviço para entregar a role a ele. Erros de cannot be assumed apontam para a trust policy.

✗ B) Incorreta. AWSLambdaBasicExecutionRole é uma política de permissão para gravar logs no CloudWatch Logs; quem pode assumir a role é definido pela trust policy, não por políticas de permissão.

✗ C) Incorreta. A resource-based policy da função controla quem pode invocá-la; ela não tem relação com o serviço Lambda assumir a role de execução.

✗ D) Incorreta. O Lambda assume a role de execução por conta própria quando a função é invocada; o usuário do pipeline só precisa de iam:PassRole, que já tem.

> **Dica de prova:** Role cannot be assumed by Lambda: trust policy sem lambda.amazonaws.com. Erro de iam:PassRole: falta permissão para quem faz o deploy.

D12. A) Allow em s3:GetObject para o Principal "*" com a condição StringEquals aws:PrincipalOrgID igual ao ID da organização no recurso do bucket de pacotes → revise o capítulo 4

Por quê: A chave global aws:PrincipalOrgID permite escrever políticas de recurso que liberam acesso a todos os principais das contas de uma organização do AWS Organizations, acompanhando automaticamente a entrada e a saída de contas. aws:PrincipalOrgPaths serve para limitar a OUs específicas, e aws:SourceOrgID e aws:SourceOrgPaths valem para chamadas de principais de serviço.

✗ B) Incorreta. aws:SourceOrgID identifica a organização do recurso de origem em chamadas feitas por principais de serviço da AWS; ela não identifica a organização de um usuário ou role que faz a requisição.

✗ C) Incorreta. Conceder acesso à conta de gerenciamento não se estende às contas membro; cada conta é um limite de segurança separado.

✗ D) Incorreta. aws:PrincipalOrgPaths restringiria o acesso aos principais da OU de produção, deixando de fora as contas das demais OUs que também precisam dos pacotes.

> **Dica de prova:** Liberar recurso para toda a organização sem lista de contas: aws:PrincipalOrgID. Para OUs específicas: aws:PrincipalOrgPaths.

Agora, treine no formato real

Faça as 6 provas completas do curso SCS-C03: 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.