Questão 1: Taxas de Transferência de Dados para Réplicas de Leitura do Amazon RDS
Resposta: Há taxas de transferência de dados para replicar dados entre regiões da AWS.
Motivo: A replicação de dados entre regiões da AWS incorre em custos de transferência de dados, ao contrário da replicação dentro da mesma região.

Questão 2: Isolamento de Instâncias EC2 de Locatário Único
Resposta: Instâncias Dedicadas.
Motivo: Instâncias Dedicadas executam em hardware dedicado a um único cliente, sendo a forma mais econômica para isolamento de locatário único em uma VPC.

Questão 3: Compartilhamento Seguro de Banco de Dados RDS
Resposta: Crie um instantâneo criptografado do banco de dados, compartilhe o instantâneo e permita o acesso à chave de criptografia do AWS Key Management Service (AWS KMS).
Motivo: Um instantâneo criptografado fornece uma cópia segura do banco de dados, e o acesso à chave KMS permite a descriptografia pelo auditor.

Questão 4: Controle de Acesso de Bucket Amazon S3 (Inter-contas)
Resposta: Usar políticas de bucket do Amazon S3.
Motivo: As políticas de bucket S3 permitem conceder ou negar permissões centralizadamente para usuários da mesma conta ou de outras contas AWS, incluindo restrições por condição.

Questão 5: Permissões de Objeto Amazon S3 para Dados Descarregados pelo Redshift

Resposta: Por padrão, um objeto Amazon S3 é de propriedade da conta AWS que o carregou.
Motivo: A propriedade do objeto S3 é da conta que o carregou, não do proprietário do bucket, exigindo uma função IAM com permissões inter-contas para acesso.

Questão 6: Otimização de Custo de Instâncias EC2 para Cargas de Trabalho Mistas
Resposta: Compre 80 instâncias reservadas (RIs). Provisione instâncias adicionais sob demanda e spot conforme a demanda da carga de trabalho.
Motivo: RIs cobrem a demanda estável, enquanto instâncias sob demanda e spot (via Auto Scaling) lidam com picos de forma econômica para cargas de trabalho de big data.

Questão 7: Alta Disponibilidade de Aplicativo EC2 com Custo Mínimo
Resposta: Implante as instâncias em três Zonas de Disponibilidade (AZs). Inicie duas instâncias em cada Zona de Disponibilidade (AZ).
Motivo: Distribuir instâncias em três AZs garante que o requisito mínimo de 4 instâncias disponíveis seja mantido mesmo se uma AZ falhar.

Questão 8: Migração de Backups On-premises para Arquivamento de Longo Prazo
Resposta: Crie um trabalho do AWS Snowball e direcione um bucket do Amazon S3. Crie uma política de ciclo de vida para fazer a transição desses dados para o Amazon S3 Glacier Deep Archive no mesmo dia.
Motivo: Snowball migra para S3, e uma política de ciclo de vida de "dia zero" move imediatamente os dados para a classe de armazenamento mais barata para arquivamento.

Questão 9: Modo de Desempenho do Amazon EFS para Big Data
Resposta: Máx. E/S.
Motivo: O modo Max I/O é otimizado para cargas de trabalho altamente paralelizadas como big data, escalando para maior throughput e operações por segundo, com uma ligeira latência em metadados.

Questão 10: Política IAM com aws:RequestedRegion

Resposta: Ele permite executar instâncias do Amazon EC2 apenas na eu-west-1 região, e a chamada da API pode ser feita de qualquer lugar do mundo.
Motivo: A condição aws:RequestedRegion restringe a ação à região especificada (eu-west-1), mas a origem da chamada da API pode ser global.

Questão 11: Melhoria de Disponibilidade de Aplicativo de Duas Camadas
Resposta: Implante as instâncias do Amazon EC2 da camada da Web em duas Zonas de Disponibilidade (AZs), atrás de um Elastic Load Balancer. Implante o banco de dados MySQL do Amazon RDS na configuração Multi-AZ.
Motivo: O Elastic Load Balancing e instâncias EC2 em múltiplas AZs para a camada web, e o RDS Multi-AZ para o banco de dados, garantem alta disponibilidade para ambas as camadas.

Questão 12: Redução de Sobrecarga e Custos com Serviços Compartilhados em VPCs
Resposta: Crie uma Amazon Virtual Private Cloud (Amazon VPC) de serviços compartilhados.
Motivo: Uma "VPC de serviços compartilhados" centraliza serviços para diversas VPCs, reduzindo sobrecarga administrativa e custos, e VPC Endpoints mantêm o tráfego na rede Amazon....

Questão 13: Solução de Problemas de Encerramento de Instância do Auto Scaling Group
Resposta: A instância pode estar em status prejudicado; O período de carência da verificação de integridade da instância não expirou; A instância falhou na verificação de status de integridade do Elastic Load Balancing (ELB).
Motivo: O ASG não encerra instâncias se o período de carência não expirou, se estão em estado 'Impaired' (aguardando recuperação), ou se as verificações de integridade do ELB falham, mas a configuração do ASG não usa o ELB para integridade.

Questão 14: Conectividade de Múltiplas VPCs e Redes Locais em Topologia Estrela
Resposta: Gateway de trânsito da AWS.
Motivo: O AWS Transit Gateway atua como um hub central, simplificando o roteamento entre múltiplas VPCs e conexões locais em uma arquitetura de rede estrela.

Questão 15: Dimensionamento Automático de Armazenamento para RDS MySQL
Resposta: Habilitar dimensionamento automático de armazenamento para Amazon RDS MySQL.
Motivo: O dimensionamento automático do RDS expande o armazenamento quando o espaço livre diminui, com mínimo esforço administrativo para cargas de trabalho imprevisíveis

Questão 16: Hospedagem de Site Estático Sem Servidor e de Alto Desempenho
Resposta: Crie o site como um site estático hospedado no Amazon S3. Crie uma distribuição do Amazon CloudFront com o Amazon S3 como origem. Use o Amazon Route 53 para criar um registro de alias que aponte para sua distribuição do Amazon CloudFront.
Motivo: S3 hospeda sites estáticos de forma econômica, CloudFront (CDN) oferece entrega global de baixa latência e Route 53 simplifica o roteamento de DNS.

Questão 17: Sistema de Arquivos de Rede Econômico para Acesso Variável
Resposta: Acesso pouco frequente do Amazon EFS.
Motivo: O EFS Infrequent Access (IA) é uma classe de armazenamento que reduz drasticamente os custos para arquivos não acessados diariamente, mantendo a compatibilidade NFS e a disponibilidade.

Questão 18: Criptografia de Bancos de Dados RDS Não Criptografados Existentes
Resposta: Tire um snapshot do banco de dados, copie-o como um snapshot criptografado e restaure um banco de dados do snapshot criptografado. Encerre o banco de dados anterior.
Motivo: A criptografia do RDS só pode ser habilitada na criação. Copiar um snapshot não criptografado para uma versão criptografada e restaurar a partir dela é a maneira de adicionar criptografia a um DB existente.

Questão 19: Separação de Requisições de Leitura e Escrita em Amazon Aurora
Resposta: Configure uma réplica de leitura e modifique o aplicativo para usar o ponto de extremidade apropriado.
Motivo: As réplicas do Aurora descarregam cargas de trabalho de leitura, permitindo que a instância primária se concentre em gravações, reduzindo a latência para as requisições de escrita.

Questão 20: Ambiente de Failover Híbrido com Mínimo Tempo de Inatividade
Resposta: Configurar um registro de failover do Amazon Route 53. Executar servidores de aplicativos em instâncias do Amazon EC2 por trás de um Application Load Balancer em um grupo de Auto Scaling. Configurar o AWS Storage Gateway com volumes armazenados para fazer backup de dados no Amazon S3.
Motivo: Route 53 e ALB/ASG proporcionam roteamento de tráfego e escalabilidade em caso de falha. Storage Gateway com volumes armazenados replica dados on-premises para S3, mantendo a uniformidade e baixa latência.

Questão 21: Latência Global de Leitura/Escrita para Amazon Aurora MySQL
Resposta: Use o Amazon Aurora Global Database para habilitar leituras locais rápidas com baixa latência em cada região.
Motivo: O Aurora Global Database estende o banco de dados por várias regiões, oferecendo leituras locais rápidas e baixa latência para aplicativos distribuídos globalmente.

Questão 22: Política IAM para Acesso Somente Leitura ao Bucket S3
Resposta: A política JSON fornecida permite s3:ListBucket no bucket e s3:GetObject nos objetos dentro do bucket.
Motivo: s3:ListBucket permite listar o conteúdo do bucket e s3:GetObject permite recuperar objetos, configurando o acesso somente leitura.

Questão 23: Criptografia S3 com Chaves Gerenciadas Pelo Cliente Localmente
Resposta: Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).
Motivo: SSE-C permite que o cliente forneça suas próprias chaves de criptografia para o S3 gerenciar a criptografia, atendendo ao requisito de chaves armazenadas em aplicativo personalizado on-premises.

Questão 24: Processamento de Dados de Telemetria Ordenados e Escaláveis
Resposta: Use uma fila FIFO (First-In-First-Out) do Amazon Simple Queue Service (Amazon SQS) e certifique-se de que os dados de telemetria sejam enviados com um atributo de ID de grupo que representa o valor do ID da área de trabalho.
Motivo: As filas SQS FIFO garantem ordem exata e processamento uma vez. O atributo GroupID permite que múltiplos consumidores processem dados em paralelo, mantendo a ordem por grupo.

Questão 25: Armazenamento Seguro e Rotação Automática de Senhas de Banco de Dados
Resposta: Gerenciador de segredos da AWS.
Motivo: O AWS Secrets Manager é projetado para armazenar, gerenciar e rotacionar credenciais de banco de dados, com integração automática para Amazon RDS.

Questão 26: Armazenamento de Data Lake Econômico com Conformidade e Consultas Ad-hoc
Resposta: Configurar uma política de ciclo de vida para fazer a transição dos dados da zona bruta para o Amazon S3 Glacier Deep Archive após 1 dia da criação do objeto; Use o trabalho ETL do AWS Glue para gravar os dados transformados na zona refinada usando um formato de arquivo compactado.
Motivo: A política de ciclo de vida move dados brutos para o armazenamento de arquivamento mais barato para conformidade. Dados refinados são compactados pelo Glue para reduzir custos de armazenamento sem impactar as consultas ad-hoc.

Questão 27: Configuração de VPC para Zonas Hospedadas Privadas do Route 53
Resposta: Habilitar nomes de host DNS e resolução DNS para zonas hospedadas privadas.

Motivo: Ambas as opções de configuração da VPC (Nomes de host DNS e Resolução de DNS) devem estar habilitadas para que as zonas hospedadas privadas funcionem corretamente com o servidor DNS da VPC

Questão 28: Armazenamento de Arquivos Econômico e Acesso Concorrente para EC2
Resposta: Amazon Elastic File System (EFS) Standard-IA storage class.
Motivo: EFS Standard-IA otimiza custos para arquivos acessados com menos frequência, enquanto o EFS oferece acesso simultâneo a milhares de instâncias EC2 e semântica de sistema de arquivos.

Questão 29: Minimizando o Tempo de Inicialização (Bootstrap) de Instâncias EC2
Resposta: Usar a hibernação da instância do Amazon EC2.
Motivo: A hibernação salva o conteúdo da RAM e o estado da instância para o EBS, permitindo que a instância retome com o aplicativo já em execução, reduzindo significativamente o tempo de inicialização.

Questão 30: Configuração de Dados do Usuário do Amazon EC2
Resposta: Por padrão, os scripts inseridos como dados do usuário são executados com privilégios de usuário root56; Por padrão, os dados do usuário são executados apenas durante o ciclo de inicialização quando você inicia uma instância pela primeira vez.
Motivo: Scripts de dados do usuário rodam como root por padrão e são executados apenas na primeira inicialização da instância (a menos que configurado de outra forma).

Questão 31: Política Padrão de Encerramento do Auto Scaling Group
Resposta: Instância B.
Motivo: A política de encerramento padrão do ASG prioriza a instância com a configuração de inicialização mais antiga antes de outros critérios.

Questão 32: Provisionamento de Capacidade em Vários Tipos de Instância com Instâncias Sob Demanda e Spot
Resposta: Você só pode usar um modelo de inicialização para provisionar capacidade em vários tipos de instância usando instâncias sob demanda e instâncias spot para atingir a escala, o desempenho e o custo desejados.
Motivo: Modelos de inicialização permitem especificar uma mistura de instâncias sob demanda e spot e diferentes tipos de instância, ao contrário das configurações de inicialização.

Questão 33: Carga de Trabalho ETL Distribuída Altamente Disponível no EC2
Resposta: Grupo de posicionamento de partição.
Motivo: Grupos de posicionamento de partição distribuem instâncias em partições lógicas para não compartilharem hardware subjacente, ideal para cargas de trabalho distribuídas e replicadas como Hadoop.

Questão 34: Conectividade EC2 com Security Groups e Network ACLs
Resposta: Os grupos de segurança são stateful, então permitir tráfego de entrada para as portas necessárias habilita a conexão. A lista de controle de acesso à rede (ACL de rede) é stateless, então você deve permitir tráfego de entrada e saída.
Motivo: Grupos de segurança são stateful (respostas de saída são automaticamente permitidas), mas ACLs de rede são stateless e exigem regras explícitas para tráfego de entrada e saída, incluindo portas efêmeras.

Questão 35: Interrupção de Ataques Baseados em Endereço IP em Aplicativos Web
Resposta: Crie uma condição de correspondência de IP no AWS WAF para bloquear o endereço IP malicioso.
Motivo: O AWS WAF permite criar regras para bloquear ou permitir solicitações web com base em endereços IP de origem, protegendo contra padrões de ataque.

Questão 36: Acesso Seguro do EC2 ao S3 e DynamoDB
Resposta: Anexe a função IAM apropriada ao perfil da instância do Amazon EC2 para que a instância possa acessar o Amazon S3 e o Amazon DynamoDB.

Motivo: Usar funções IAM com perfis de instância fornece credenciais temporárias para aplicativos no EC2, eliminando a necessidade de gerenciar credenciais de longo prazo.

Questão 37: Melhoria de Desempenho Global de Aplicativos Web com Aurora
Resposta: Crie réplicas de leitura do Amazon Aurora na eu-west-1 região; Configure outra frota de instâncias do Amazon EC2 para a camada da web na eu-west-1 região. Habilite a política de roteamento de latência no Amazon Route 53.
Motivo: Implantar recursos web e réplicas de leitura do Aurora em uma região mais próxima (eu-west-1) e usar o roteamento baseado em latência do Route 53 direciona o tráfego para o endpoint de menor latência, melhorando o desempenho para usuários europeus.

Questão 38: Otimização de Custo para Frota de Instâncias EC2 Mistas
Resposta: Compre 70 instâncias reservadas (RIs) e 30 instâncias spot.
Motivo: RIs são ideais para cargas de trabalho estáveis que precisam estar sempre disponíveis. Spot Instances são econômicas para cargas de trabalho em lote que podem tolerar interrupções.

Questão 39: Criptografia de Réplicas de Leitura do Amazon RDS
Motivo: A criptografia em repouso de uma instância de banco de dados RDS se estende automaticamente aos seus backups, snapshots e réplicas de leitura.

Questão 40: Replicação de Dados S3 Criptografados Entre Regiões com Chave Consistente
Resposta: Crie um novo bucket do Amazon S3 na us-east-1 região com replicação habilitada deste novo bucket para outro bucket na us-west-1 região. Habilite a criptografia SSE-KMS no novo bucket na us-east-1 região usando uma chave multirregional do AWS KMS. Copie os dados existentes do bucket atual do Amazon S3 na us-east-1 região para este novo bucket do Amazon S3 na us-east-1 região....
Motivo: Chaves KMS multirregionais permitem criptografia e descriptografia consistentes entre regiões. Habilitar a replicação para um novo bucket com essa chave garante a disponibilidade e criptografia uniforme para DR.

Questão 41: Tecnologia de Banco de Dados para Sobrescritas/Exclusões Frequentes e Consistência Forte
Resposta: Serviço de banco de dados relacional da Amazon (Amazon RDS).
Motivo: O Amazon RDS garante propriedades ACID, o que é crucial para aplicações que exigem que as informações mais recentes estejam sempre disponíveis após operações frequentes de gravação e exclusão.

Questão 42: Criptografia S3 com Auditoria e Rotação Anual de Chaves
Resposta: Criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) com rotação automática de chaves8485.
Motivo: SSE-KMS permite gerenciar chaves centralizadamente, registrar o uso para auditoria e oferece rotação automática de chaves anualmente, atendendo aos requisitos de segurança e conformidade8586.

Questão 43: Envio de Dados do Kinesis Agent para Firehose com Kinesis Data Streams como Origem
Resposta: O Kinesis Agent não pode gravar no Amazon Kinesis Firehose para o qual a origem do fluxo de entrega já está definida como Amazon Kinesis Data Streams.
Motivo: Se o Firehose estiver configurado para receber dados de um Kinesis Data Stream, as operações de PutRecord/PutRecordBatch (usadas pelo Agent) são desabilitadas; os dados devem ser enviados primeiro para o Kinesis Data Stream.

Questão 44: Notificação de Certificados SSL/TLS de Terceiros Expirando no ACM
Resposta: Aproveite a regra gerenciada do AWS Config para verificar se algum certificado SSL/TLS de terceiros importado para o ACM está marcado para expiração em 30 dias. Configure a regra para disparar uma notificação do Amazon SNS para a equipe de segurança se algum certificado expirar em 30 dias.

Motivo: Regras gerenciadas do AWS Config podem monitorar certificados importados (que não são renovados automaticamente pelo ACM) e enviar notificações via SNS, com mínimo esforço de script.

Questão 45: Persistência do Volume Raiz do EBS Após Encerramento da Instância EC2
Resposta: Defina o DeleteOnTermination atributo como falso.
Motivo: Por padrão, o volume raiz do EBS é excluído ao encerrar a instância. Definir DeleteOnTermination como falso garante que o volume persista.

Questão 46: Processamento e Armazenamento Confiável de Dados de Telemetria de Chave-Valor
Resposta: Amazon DynamoDB; AWS Lambda.
Motivo: AWS Lambda oferece processamento serverless e escalável para os dados de telemetria, enquanto o DynamoDB é um banco de dados NoSQL de chave-valor, totalmente gerenciado, que oferece desempenho em milissegundos e alta disponibilidade.

Questão 47: Configuração de Grupos de Segurança para Aplicativo de 3 Camadas
Resposta: O grupo de segurança do Application Load Balancer deve ter uma regra de entrada de qualquer lugar na porta 443; O grupo de segurança do Amazon RDS deve ter uma regra de entrada do grupo de segurança das instâncias do Amazon EC2 no grupo de dimensionamento automático na porta 543; O grupo de segurança das instâncias do Amazon EC2 deve ter uma regra de entrada do grupo de segurança do Application Load Balancer na porta 80.
Motivo: Essas regras estabelecem um fluxo de tráfego seguro: Internet para ALB (443), ALB para EC2 (80) e EC2 para RDS (5432), utilizando referências a grupos de segurança para segurança entre componentes.

Questão 48: Autenticação/Autorização para API Gateway com Gerenciamento de Usuário Integrado
Resposta: Use pools de usuários do Amazon Cognito.
Motivo: Os Pools de Usuários do Amazon Cognito fornecem um diretório de usuários integrado e serviços de inscrição/login, e podem ser usados como autorizadores no API Gateway.

Questão 49: Carga de Trabalho Big Data Mensal e Tolerante a Falhas de Baixo Custo
Resposta: Execute a carga de trabalho em uma frota Spot.
Motivo: Spot Fleets permitem usar instâncias Spot não utilizadas a um custo significativamente menor, ideais para cargas de trabalho flexíveis e tolerantes a falhas que podem ser distribuídas.

Questão 50: Armazenamento Otimizado para Vídeos Carregados por Usuários em Serviço Web
Resposta: Escreva um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon S3 e, em seguida, modifique o aplicativo para usar o padrão Amazon S3 para armazenar os vídeos; Monte o Amazon Elastic File System (Amazon EFS) em todas as instâncias do Amazon EC2. Grave um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon EFS. Modifique o aplicativo para usar o Amazon EFS para armazenar os vídeos.
Motivo: Volumes EBS são locais a instâncias específicas, causando dados dispersos. S3 (armazenamento de objetos) ou EFS (sistema de arquivos compartilhado) são soluções de armazenamento centralizado que permitem que todas as instâncias acessem os mesmos vídeos.

Questão 51: Baixa Latência Global de Leitura/Escrita em Amazon Aurora com RPO/RTO Específicos
Resposta: Configurar um cluster do Amazon Aurora Global Database.
Motivo: O Aurora Global Database é projetado para aplicativos distribuídos globalmente, oferecendo leituras/escritas de baixa latência e recuperação de desastres com RPO de segundos e RTO de menos de 1 minuto em caso de interrupção regional.

Questão 52: Melhoria de Escala de Leitura e Disponibilidade do Aurora e Criação de DB de Desenvolvimento
Resposta: Aproveite o Amazon Aurora MySQL com réplicas Multi-AZ Aurora e crie o banco de dados dev restaurando a partir dos backups automatizados do Amazon Aurora.

Motivo: As réplicas Multi-AZ do Aurora melhoram a escalabilidade de leitura e a disponibilidade. Backups automatizados contínuos do Aurora permitem a restauração de um DB de desenvolvimento sem impacto no desempenho da produção.

Questão 53: Replicação de Arquivos de Vídeo Locais para Amazon EFS via Direct Connect

Resposta: Configure um agente AWS DataSync no servidor local que tenha acesso ao sistema de arquivos NFS. Transfira dados pela conexão AWS Direct Connect para um endpoint VPC da interface AWS PrivateLink para Amazon EFS usando um VIF privado. Configure uma tarefa agendada do AWS DataSync para enviar os arquivos de vídeo para o sistema de arquivos Amazon EFS a cada 24 horas.

Motivo: O AWS DataSync automatiza e acelera a transferência de dados de NFS on-premises para EFS, usando Direct Connect e PrivateLink para uma conexão privada e eficiente.

Questão 54: Migração de Conta AWS Entre Organizações AWS

Resposta: Remova a conta de membro da organização antiga. Envie um convite para a conta de membro da nova organização. Aceite o convite para a nova organização da conta de membro.

Motivo: O processo padrão para migrar uma conta entre organizações envolve desvinculá-la da organização atual, enviar um novo convite e aceitá-lo.

Questão 55: Implantação Blue/Green com Problemas de Cache DNS para Transição Rápida

Resposta: Use o AWS Global Accelerator para distribuir uma parte do tráfego para uma implantação específica.

Motivo: O Global Accelerator permite o roteamento de tráfego rápido e controlado entre ambientes Blue/Green usando IPs anycast estáticos e pesos/controles de tráfego, evitando o impacto do cache DNS do cliente.

Questão 56: Análise de Política IAM com Condições de Negação por Região e Permissão por IP

Resposta: Usuários pertencentes ao grupo de usuários do IAM podem encerrar uma instância do Amazon EC2 na us-west-1 região quando o IP de origem do usuário for 10.200.200.200.

Motivo: A política nega todas as ações EC2 fora de us-west-1. Dentro de us-west-1, ela permite TerminateInstances apenas para o IP de origem especificado.

Questão 57: Desacoplamento da Autenticação de Usuário para Aplicativo Web

Resposta: Use a autenticação do Amazon Cognito por meio de pools de usuários do Cognito para seu balanceador de carga de aplicativo.

Motivo: O ALB pode integrar-se diretamente com os Pools de Usuários do Amazon Cognito para autenticar usuários, aliviando essa carga dos servidores de aplicação com mínimo esforço de desenvolvimento.

Questão 58: Notificação de Utilização da CPU do EC2 Via Email com Mínimo Esforço

Resposta: Amazon CloudWatch; Serviço de notificação simples da Amazon (Amazon SNS).

Motivo: O Amazon CloudWatch monitora métricas do EC2 e pode disparar alarmes que, por sua vez, enviam notificações por e-mail via Amazon SNS, fornecendo uma solução gerenciada.

Questão 59: Função Lambda em Conta A Acessando Bucket S3 em Conta B

Resposta: Crie uma função do IAM para a função do AWS Lambda que conceda acesso ao bucket do Amazon S3. Defina a função do IAM como a função de execução da função do AWS Lambda. Certifique-se de que a política do bucket também conceda acesso à função de execução da função do AWS Lambda.

Motivo: Para acesso inter-contas, tanto a função IAM da Lambda quanto a política do bucket S3 devem conceder permissões explicitamente à função de execução da Lambda.

Questão 60: Prevenção de Escalada de Privilégios de Desenvolvedores IAM

Resposta: Para cada desenvolvedor, defina um limite de permissão do IAM que restringirá as políticas gerenciadas que eles podem anexar a si mesmos.

Motivo: Um limite de permissões IAM define as permissões máximas que uma política baseada em identidade pode conceder a uma entidade IAM, impedindo a escalada de privilégios.

Questão 61: Comunicação Privada entre Instâncias EC2 em Múltiplas Contas AWS (Mesma Região)
Resposta: Crie uma nuvem privada virtual (VPC) em uma conta e compartilhe uma ou mais de suas sub-redes com as outras contas usando o Resource Access Manager.
Motivo: O AWS RAM permite compartilhar sub-redes VPC entre contas dentro de uma Organização, permitindo que instâncias de diferentes contas se comuniquem privadamente na mesma VPC sem custo adicional.

Questão 62: Substituição para DFSR Local em Servidores Windows
Resposta: Amazon FSx para servidor de arquivos do Windows.
Motivo: O Amazon FSx para Windows File Server é um serviço de arquivo gerenciado que suporta o protocolo SMB e o Distributed File System (DFS), sendo um substituto direto para o DFSR local.

Questão 63: Configuração de Segurança para Aplicativo de Duas Camadas com Servidores Web e DB MSSQL
Resposta: Para o grupo de segurança B: adicione uma regra de entrada que permita tráfego somente do grupo de segurança A na porta 1433; Para o grupo de segurança A: adicione uma regra de entrada que permita tráfego de todas as origens na porta 443. Adicione uma regra de saída com o destino como grupo de segurança B na porta 1433.
Motivo: Esta configuração garante que os servidores web recebam tráfego HTTPS e que somente os servidores web possam acessar o banco de dados MSSQL na porta 1433, criando uma comunicação segura entre as camadas.

Questão 64: Processamento e Armazenamento de Logs Serverless e Escalável
Resposta: Amazon Kinesis Data Firehose.
Motivo: O Kinesis Data Firehose é um serviço totalmente gerenciado que escala automaticamente para lidar com dados de streaming (incluindo logs), e pode carregá-los de forma confiável para armazenamento e ferramentas de análise, sem administração contínua.

Questão 65: Análise de Política IAM com Condição de IP de Origem
Resposta: Ele permite iniciar uma instância do Amazon EC2 somente quando o IP de onde a chamada se origina está dentro do 34.50.31.0/24 bloco CIDR.
Motivo: A condição aws:SourceIp restringe a execução de instâncias EC2 apenas a chamadas de API que se originam de um endereço IP dentro do bloco CIDR especificado.