

### Pergunta 1

Um desenvolvedor configurou o tráfego de entrada para as portas relevantes tanto no Grupo de Segurança da instância do Amazon EC2 quanto na Lista de Controle de Acesso à Rede (ACL de Rede) da sub-rede da instância do Amazon EC2. No entanto, o desenvolvedor não consegue se conectar ao serviço em execução na instância do Amazon EC2.

Como arquiteto de soluções, como você resolverá esse problema?

**R: Os Grupos de Segurança têm estado, portanto, permitir o tráfego de entrada nas portas necessárias habilita a conexão. As ACLs de rede não têm estado, portanto, você deve permitir o tráfego de entrada e saída.**

**Opção correta:**

**Os Grupos de Segurança têm estado, portanto, permitir o tráfego de entrada nas portas necessárias habilita a conexão. As ACLs de rede não têm estado, portanto, você deve permitir o tráfego de entrada e saída.**

Os grupos de segurança têm estado, portanto, permitir o tráfego de entrada nas portas necessárias habilita a conexão. As ACLs de rede não têm estado, portanto, você deve permitir tanto o tráfego de entrada quanto o de saída.

Para habilitar a conexão com um serviço em execução em uma instância, a ACL de rede associada deve permitir tanto o tráfego de entrada na porta em que o serviço está escutando quanto o tráfego de saída de portas efêmeras. Quando um cliente se conecta a um servidor, uma porta aleatória do intervalo de portas efêmeras (1024-65535) se torna a porta de origem do cliente.

A porta efêmera designada se torna então a porta de destino para o tráfego de retorno do serviço, portanto, o tráfego de saída da porta efêmera deve ser permitido na ACL da rede.

Por padrão, as ACLs de rede permitem todo o tráfego de entrada e saída. Se a sua ACL de rede for mais restritiva, você precisará permitir explicitamente o tráfego do intervalo de portas efêmeras.

Se você aceitar tráfego da internet, também deverá estabelecer uma rota por meio de um gateway de internet. Se você aceitar tráfego via VPN ou AWS Direct Connect, deverá estabelecer uma rota por meio de um gateway privado virtual (VGW).

### Pergunta 2

A equipe de DevOps de uma empresa de TI migrou recentemente para a AWS e está configurando grupos de segurança para sua aplicação de duas camadas com servidores web públicos e servidores de banco de dados privados. A equipe deseja entender as opções de configuração permitidas para uma regra de entrada para um grupo de segurança.

Como arquiteto de soluções, qual das seguintes opções você identificaria como uma opção INVÁLIDA para configurar tal configuração?

**R: Você pode usar um ID de gateway da Internet como fonte personalizada para a regra de entrada**

**Opção correta:**

**Você pode usar um ID de gateway da Internet como fonte personalizada para a regra de entrada**

Um grupo de segurança atua como um firewall virtual que controla o tráfego de uma ou mais instâncias. Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança; caso contrário, pode usar o grupo de segurança padrão. Você pode adicionar regras a cada grupo de segurança que permitam o tráfego de ou para suas instâncias associadas. Você pode modificar as regras de um grupo de segurança a qualquer momento; as novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

um ID de gateway da Internet como fonte personalizada para a regra de entrada.

### Pergunta 3

Uma empresa de treinamento em TI hospedou seu site no Amazon S3 há alguns anos. Devido às restrições de viagens relacionadas à COVID-19, o site de treinamento ganhou força repentinamente. Com um aumento de quase 300% nas solicitações atendidas por dia, os custos da empresa com a AWS dispararam, considerando apenas os custos de dados de saída do Amazon S3.

Como arquiteto de soluções, você pode sugerir um método alternativo para reduzir custos e manter a latência baixa?

**R: Configure o Amazon CloudFront para distribuir os dados hospedados no Amazon S3 de forma econômica**

**Opção correta:**

**Configure o Amazon CloudFront para distribuir os dados hospedados no Amazon S3 de forma econômica**

Armazenar conteúdo com o Amazon S3 oferece muitas vantagens. Mas para ajudar a otimizar o desempenho e a segurança do seu aplicativo, além de gerenciar custos de forma eficaz, a AWS recomenda que você também configure o Amazon CloudFront para trabalhar com o seu bucket do Amazon S3 para servir e proteger o conteúdo.

O Amazon CloudFront é um serviço de rede de distribuição de conteúdo (CDN) que distribui conteúdo web estático e dinâmico, fluxos de vídeo e APIs em todo o mundo, com segurança e em escala. Por definição, a entrega de dados do Amazon CloudFront pode ser mais econômica do que entregá-los diretamente do Amazon S3 para seus usuários.

O Amazon CloudFront disponibiliza conteúdo por meio de uma rede mundial de data centers chamada de Locais de Borda. O uso de servidores de borda para armazenar em cache e disponibilizar conteúdo melhora o desempenho, fornecendo conteúdo mais próximo de onde os espectadores estão localizados. O Amazon CloudFront possui servidores de borda em locais ao redor do mundo.

Quando um usuário solicita conteúdo que você disponibiliza com o Amazon CloudFront, a solicitação é roteada para um Edge Location próximo. Se o CloudFront tiver uma cópia em cache do arquivo solicitado, ele a entregará ao usuário, fornecendo uma resposta rápida (de baixa latência). Se o arquivo solicitado ainda não estiver em cache, o Amazon CloudFront o recuperará da sua origem – por exemplo, o bucket do S3 onde você armazenou seu conteúdo. Assim, para a próxima solicitação local do mesmo conteúdo, ele já estará em cache nas proximidades e poderá ser disponibilizado imediatamente.

Ao armazenar seu conteúdo em cache em Locais de Borda, o Amazon CloudFront reduz a carga no seu bucket do Amazon S3 e ajuda a garantir uma resposta mais rápida para seus usuários quando eles solicitam conteúdo. Além disso, a transferência de dados para conteúdo usando o CloudFront costuma ser mais econômica do que servir arquivos diretamente do Amazon S3, e não há taxa de transferência de dados do Amazon S3 para o CloudFront. Você paga apenas pelo que é entregue à internet pelo Amazon CloudFront, mais as taxas de solicitação.

#### **Pergunta 4**

Uma empresa de comércio eletrônico utiliza o Microsoft Active Directory para fornecer aos usuários e grupos acesso a recursos na infraestrutura local. A empresa estendeu sua infraestrutura de TI para a AWS na forma de uma nuvem híbrida. A equipe de engenharia da empresa deseja executar cargas de trabalho com reconhecimento de diretório na AWS para um aplicativo baseado em SQL Server. A equipe também deseja configurar uma relação de confiança para habilitar o logon único (SSO) para que seus usuários acessem recursos em qualquer um dos domínios.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você recomendaria para este caso de uso?

**R: Serviço de diretório da AWS para Microsoft Active Directory (AWS Managed Microsoft AD)**

**Opção correta:**

**Serviço de diretório da AWS para Microsoft Active Directory (AWS Managed Microsoft AD)**

O AWS Directory Service oferece diversas maneiras de usar o Amazon Cloud Directory e o Microsoft Active Directory (AD) com outros serviços da AWS.

O AWS Directory Service para Microsoft Active Directory (também conhecido como AWS Managed Microsoft AD) é alimentado por um Active Directory (AD) real do Microsoft Windows Server, gerenciado pela AWS. Com o AWS Managed Microsoft AD, você pode executar cargas de trabalho com reconhecimento de diretório na Nuvem AWS, como aplicativos baseados em SQL Server. Você também pode configurar uma relação de confiança entre o AWS Managed Microsoft AD na Nuvem AWS e seu Microsoft Active Directory local existente, fornecendo aos usuários e grupos acesso a recursos em qualquer domínio, usando logon único (SSO).

#### **Alerta de exame:**

Você poderá ver perguntas sobre a escolha entre "AWS Managed Microsoft AD" vs. "AD Connector" vs. "Simple AD" no exame. Lembre-se de que você deve usar o AD Connector se precisar permitir que seus usuários locais efetuem login em aplicativos da AWS com suas credenciais do Active Directory. O AWS Managed Microsoft AD também permite que você execute cargas de trabalho com reconhecimento de diretório na Nuvem AWS. O AWS Managed Microsoft AD é a melhor opção se você tiver mais de 5.000 usuários e precisar configurar uma relação de confiança entre um diretório hospedado na AWS e seus diretórios locais. O Simple AD é a opção mais barata e a melhor opção se você tiver 5.000 usuários ou menos e não precisar dos recursos mais avançados do Microsoft Active Directory, como relações de confiança com outros domínios.

#### **Pergunta 5**

Uma empresa criou o AWS Organizations para gerenciar diversos departamentos que administram suas próprias contas na AWS. Os departamentos operam em diferentes países e estão distribuídos por diversas regiões da AWS. A empresa deseja estabelecer um processo consistente de provisionamento de recursos entre os departamentos, de modo que cada recurso siga configurações predefinidas, como o uso de um tipo específico de instância do Amazon EC2, funções específicas do IAM para funções do AWS Lambda, etc.

Como arquiteto de soluções, qual das seguintes opções você recomendaria para este caso de uso?

**R: Use o AWS CloudFormation StackSets para implantar o mesmo modelo em contas e regiões da AWS**

**Opção correta:**

**Use o AWS CloudFormation StackSets para implantar o mesmo modelo em contas e regiões da AWS**

O AWS CloudFormation StackSet amplia a funcionalidade das pilhas, permitindo que você crie, atualize ou exclua pilhas em várias contas e regiões com uma única operação. Um conjunto de pilhas permite criar pilhas em contas da AWS em diferentes regiões usando um único modelo do AWS CloudFormation. Usando uma conta de administrador de uma "Organização da AWS", você define e gerencia um modelo do AWS CloudFormation e o usa como base para provisionar pilhas em contas de destino selecionadas de uma "Organização da AWS" em regiões especificadas.

#### **Pergunta 6**

Uma empresa de serviços financeiros migrou recentemente de uma infraestrutura local para a Nuvem AWS. A equipe de DevOps deseja implementar uma solução que permita a revisão de todas as configurações de recursos e garanta que atendam às diretrizes de conformidade. Além disso, a solução deve oferecer a capacidade de analisar o histórico de configuração de recursos em toda a pilha de aplicativos.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria à equipe?

**R: Use o AWS Config para revisar as configurações de recursos para atender às diretrizes de conformidade e manter um histórico das alterações na configuração de recursos.**

**Opção correta:**

**Use o AWS Config para revisar as configurações de recursos para atender às diretrizes de conformidade e manter um histórico das alterações na configuração de recursos.**

O AWS Config é um serviço que permite avaliar, auditar e analisar as configurações dos seus recursos da AWS. Com o Config, você pode revisar alterações nas configurações e relacionamentos entre os recursos da AWS, analisar históricos detalhados de configuração de recursos e determinar sua conformidade geral com as configurações especificadas em suas diretrizes internas. Você pode usar o Config para responder a perguntas como: "Como estava meu recurso da AWS no momento xyz?"

#### **Alerta de exame:**

Você pode ver perguntas baseadas em cenários solicitando que você selecione entre Amazon CloudWatch, AWS CloudTrail ou AWS Config. Lembre-se desta regra básica:

Pense em monitoramento de desempenho de recursos, eventos e alertas; pense no Amazon CloudWatch.

Pense em atividades e auditorias específicas de contas; pense no AWS CloudTrail.

Pense em histórico, auditoria e conformidade específicos de recursos; pense no AWS Config.

#### **Pergunta 7**

Uma empresa de varejo tem seu aplicativo principal em execução em uma frota de instâncias do Amazon EC2 por meio do Elastic Load Balancing (ELB). A equipe de engenharia tem observado problemas recorrentes em que as solicitações em andamento do ELB para as instâncias do Amazon EC2 são descartadas quando uma instância apresenta problemas de integridade.

Qual dos seguintes recursos pode ser usado para resolver esse problema?

**R: Conexão drenando**

**Opção correta:**

#### **Conexão drenando**

Para garantir que o Elastic Load Balancing pare de enviar solicitações para instâncias que estão cancelando o registro ou não estão íntegras, mantendo as conexões existentes abertas, use o esvaziamento de conexão. Isso permite que o balanceador de carga conclua solicitações em andamento feitas para instâncias que estão cancelando o registro ou não estão íntegras. O valor máximo de tempo limite pode ser definido entre 1 e 3.600 segundos (o padrão é 300 segundos). Quando o limite máximo de tempo é atingido, o balanceador de carga fecha à força as conexões para a instância que está cancelando o registro.

#### **Pergunta 8**

Uma empresa contratou você como Arquiteto de Soluções Certificado pela AWS - Associado para ajudar a redesenhar um processador de dados em tempo real. A empresa deseja criar aplicativos personalizados que processem e analisem os dados de streaming para suas necessidades específicas.

Qual solução você recomendaria para abordar esse caso de uso?

**R: Use o Amazon Kinesis Data Streams para processar os fluxos de dados, bem como desacoplar os produtores e consumidores para o processador de dados em tempo real**

**Opção correta:**

**Use o Amazon Kinesis Data Streams para processar os fluxos de dados, bem como desacoplar os produtores e consumidores para o processador de dados em tempo real**

O Amazon Kinesis Data Streams é útil para transferir dados rapidamente de produtores de dados e processá-los continuamente, seja para transformá-los antes de enviá-los para um armazenamento de dados, executar métricas e análises em tempo real ou derivar fluxos de dados mais complexos para processamento posterior. Os fluxos de dados do Kinesis podem capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de bancos de

dados, transações financeiras, feeds de mídia social, registros de TI e eventos de rastreamento de localização.

#### **Pergunta 9**

Uma empresa de serviços financeiros está buscando migrar sua infraestrutura de TI local para a Nuvem AWS. A empresa possui diversas licenças de longo prazo vinculadas ao servidor em toda a pilha de aplicativos, e o CTO deseja continuar a utilizar essas licenças durante a migração para a AWS.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução MAIS econômica?

**R: Use hosts dedicados do Amazon EC2**

**Opção correta:**

**Use hosts dedicados do Amazon EC2**

Você pode usar Hosts Dedicados para iniciar instâncias do Amazon EC2 em servidores físicos dedicados para seu uso. Hosts Dedicados oferecem visibilidade e controle adicionais sobre como as instâncias são alocadas em um servidor físico, permitindo que você use o mesmo servidor físico de forma confiável ao longo do tempo. Como resultado, os Hosts Dedicados permitem que você use suas licenças de software vinculadas ao servidor existentes, como o Windows Server, e atenda aos requisitos de conformidade corporativa e regulatórios.

#### **Pergunta 10**

Um banco líder migrou sua infraestrutura de TI para a Nuvem AWS e vem utilizando o Amazon EC2 Auto Scaling em seus servidores web. Isso os ajudou a lidar com picos de tráfego de forma eficaz. No entanto, seu banco de dados relacional MySQL se tornou um gargalo e eles precisam urgentemente de uma solução de auto escalonamento totalmente gerenciada para seu banco de dados relacional, a fim de lidar com quaisquer mudanças imprevisíveis no tráfego.

Você consegue identificar o serviço da AWS mais adequado para esse caso de uso?

**R: Amazon Aurora sem servidor**

**Opções corretas:**

**Amazon Aurora sem servidor**

O Amazon Aurora Serverless é uma configuração sob demanda e com escalonamento automático para o Amazon Aurora (edições compatíveis com MySQL e PostgreSQL), na qual o banco de dados inicia, encerra e aumenta ou diminui a capacidade automaticamente, de acordo com as necessidades do seu aplicativo. Ele permite que você execute seu banco de dados na nuvem sem precisar gerenciar nenhuma instância. É uma opção simples e econômica para cargas de trabalho pouco frequentes, intermitentes ou imprevisíveis. Você paga por segundo pela capacidade do banco de dados que utiliza quando o banco de dados está ativo e migra entre as configurações padrão e sem servidor com apenas alguns cliques no Console de Gerenciamento do Amazon RDS.

#### **Pergunta 11**

Um aplicativo de jogos online tem grande parte do seu tráfego proveniente de usuários que baixam recursos estáticos, como relatórios históricos de tabelas de classificação e táticas de jogo para diversos jogos. A infraestrutura e o design atuais não conseguem lidar com o tráfego, e o aplicativo trava na maioria das páginas.

Qual das seguintes opções é uma solução com melhor custo-benefício que não necessita de provisionamento de infraestrutura?

**R: Use o Amazon CloudFront com o Amazon S3 como solução de armazenamento para ativos estáticos**

**Opção correta:**

## **Use o Amazon CloudFront com o Amazon S3 como solução de armazenamento para ativos estáticos**

Ao colocar seu conteúdo em um bucket do Amazon S3 na nuvem, muitas coisas se tornam muito mais fáceis. Primeiro, você não precisa planejar e alocar uma quantidade específica de espaço de armazenamento, pois os buckets do Amazon S3 escalam automaticamente. Como o Amazon S3 é um serviço sem servidor, você não precisa gerenciar ou aplicar patches nos servidores que armazenam arquivos; você simplesmente coloca e recebe seu conteúdo. Por fim, mesmo que você precise de um servidor para seu aplicativo (por exemplo, porque você tem um aplicativo dinâmico), o servidor pode ser menor, pois não precisa lidar com solicitações de conteúdo estático.

O Amazon CloudFront é um serviço de rede de distribuição de conteúdo (CDN) que distribui conteúdo web estático e dinâmico, fluxos de vídeo e APIs em todo o mundo, com segurança e em escala. Por padrão, a entrega de dados do Amazon CloudFront pode ser mais econômica do que entregá-los diretamente do Amazon S3 para seus usuários. O Amazon CloudFront disponibiliza conteúdo por meio de uma rede mundial de data centers chamada de Locais de Borda. O uso de servidores de borda para armazenar em cache e disponibilizar conteúdo melhora o desempenho, fornecendo conteúdo mais próximo de onde os espectadores estão localizados.

Quando um usuário solicita conteúdo que você disponibiliza com o Amazon CloudFront, a solicitação é roteada para um Edge Location próximo. Se o Amazon CloudFront tiver uma cópia em cache do arquivo solicitado, o CloudFront a entrega ao usuário, fornecendo uma resposta rápida (de baixa latência). Se o arquivo solicitado ainda não estiver em cache, o CloudFront o recupera da sua origem – por exemplo, o bucket do Amazon S3 onde você armazenou seu conteúdo. Assim, para a próxima solicitação local do mesmo conteúdo, ele já estará em cache nas proximidades e poderá ser disponibilizado imediatamente.

Ao armazenar seu conteúdo em cache em Locais de Borda, o Amazon CloudFront reduz a carga no seu bucket do Amazon S3 e ajuda a garantir uma resposta mais rápida para seus usuários quando eles solicitam conteúdo. Além disso, a transferência de dados para conteúdo usando o Amazon CloudFront costuma ser mais econômica do que servir arquivos diretamente do Amazon S3, e não há taxa de transferência de dados do Amazon S3 para o Amazon CloudFront. Você paga apenas pelo que é entregue à internet pelo Amazon CloudFront, mais as taxas de solicitação.

### **Pergunta 12**

Uma empresa possui uma solução de banco de dados comercial legada, cara e baseada em licença, implantada em seu data center local. A empresa deseja migrar esse banco de dados para uma opção mais eficiente, de código aberto e econômica na Nuvem AWS. O CTO da empresa deseja uma solução que possa lidar com configurações complexas de banco de dados, como índices secundários, chaves estrangeiras e procedimentos armazenados.

Como arquiteto de soluções, quais dos seguintes serviços da AWS devem ser combinados para lidar com este caso de uso? (Selecione duas)

**R: Ferramenta de Conversão de Esquema da AWS (AWS SCT) R: Serviço de migração de banco de dados AWS (AWS DMS)**

**Opções corretas:**

- **Ferramenta de Conversão de Esquema da AWS (AWS SCT)**
- **Serviço de migração de banco de dados AWS (AWS DMS)**

O AWS Database Migration Service ajuda você a migrar bancos de dados para a AWS de forma rápida e segura. O banco de dados de origem permanece totalmente operacional durante a migração, minimizando o tempo de inatividade para aplicativos que dependem do banco de dados. O AWS Database Migration Service oferece suporte a migrações homogêneas, como Oracle para Oracle, bem como migrações heterogêneas entre diferentes plataformas de banco de dados, como Oracle ou Microsoft SQL Server para Amazon Aurora.

Dado o caso de uso em que o CTO da empresa quer migrar de soluções de banco de dados comerciais legadas, caras e baseadas em licenças, implantadas no data center local para opções mais eficientes, de código aberto e econômicas na Nuvem AWS, este é um exemplo de migrações heterogêneas de banco de dados.

Nesse cenário, os mecanismos dos bancos de dados de origem e de destino são diferentes, como no caso de migrações do Oracle para o Amazon Aurora, do Oracle para o PostgreSQL ou do Microsoft SQL Server para o MySQL. Nesse caso, a estrutura do esquema, os tipos de dados e o código dos bancos de dados de origem e de destino podem ser bem diferentes, exigindo uma transformação do esquema e do código antes do início da migração dos dados.

Isso torna as migrações heterogêneas um processo de duas etapas. Primeiro, use a AWS Schema Conversion Tool para converter o esquema e o código de origem para corresponder aos do banco de dados de destino e, em seguida, use o AWS Database Migration Service para migrar os dados do banco de dados de origem para o banco de dados de destino. Todas as conversões de tipo de dados necessárias serão realizadas automaticamente pelo AWS Database Migration Service durante a migração. O banco de dados de origem pode estar localizado em seu ambiente local fora da AWS, em execução em uma instância do Amazon EC2, ou pode ser um banco de dados do Amazon RDS. O destino pode ser um banco de dados no Amazon EC2 ou no Amazon RDS.

### **Pergunta 13**

A equipe de engenharia de uma empresa de comércio eletrônico deseja migrar das filas do Amazon Simple Queue Service (Amazon SQS) Standard para filas FIFO (First-In-First-Out) com lotes.

Como arquiteto de soluções, qual das seguintes etapas você incluiria na lista de verificação de migração? (Selecione três)

**R: Certifique-se de que o nome da fila FIFO (First-In-First-Out) termina com o sufixo .fifo**

**R: Certifique-se de que a taxa de transferência da fila FIFO (First-In-First-Out) de destino não exceda 3.000 mensagens por segundo**

**R: Exclua a fila padrão existente e recrie-a como uma fila FIFO (First-In-First-Out)**

**Opções corretas:**

- **Exclua a fila padrão existente e recrie-a como uma fila FIFO (First-In-First-Out)**
- **Certifique-se de que o nome da fila FIFO (First-In-First-Out) termina com o sufixo .fifo**
- **Certifique-se de que a taxa de transferência da fila FIFO (First-In-First-Out) de destino não exceda 3.000 mensagens por segundo**

O Amazon Simple Queue Service (SQS) é um serviço de enfileiramento de mensagens totalmente gerenciado que permite desacoplar e escalar microsserviços, sistemas distribuídos e aplicações sem servidor. O Amazon SQS elimina a complexidade e a sobrecarga associadas ao gerenciamento e operação de middleware orientado a mensagens e permite que os desenvolvedores se concentrem na diferenciação do trabalho. Com o Amazon SQS, você pode enviar, armazenar e receber mensagens entre componentes de software em qualquer volume, sem perder mensagens ou exigir a disponibilidade de outros serviços.

O Amazon SQS oferece dois tipos de filas de mensagens. As filas padrão oferecem taxa de transferência máxima, ordenação de melhor esforço e entrega pelo menos uma vez. As filas FIFO do SQS são projetadas para garantir que as mensagens sejam processadas exatamente uma vez, na ordem exata em que são enviadas.

Por padrão, as filas FIFO suportam até 3.000 mensagens por segundo com processamento em lote, ou até 300 mensagens por segundo (300 operações de envio, recebimento ou exclusão por segundo) sem processamento em lote. Portanto, com o processamento em lote, você pode atender a um requisito de throughput de até 3.000 mensagens por segundo.

O nome de uma fila FIFO deve terminar com o sufixo .fifo. O sufixo conta para o limite de 80 caracteres para nomes de fila. Para determinar se uma fila é FIFO, você pode verificar se o nome da fila termina com o sufixo.

Se você já possui um aplicativo que utiliza filas padrão e deseja aproveitar os recursos de ordenação ou processamento exatamente único das filas FIFO, precisa configurar a fila e o aplicativo corretamente. Não é possível converter uma fila

padrão existente em uma fila FIFO. Para fazer isso, você precisa criar uma nova fila FIFO para o seu aplicativo ou excluir a fila padrão existente e recriá-la como uma fila FIFO.

#### **Pergunta 14**

Uma empresa de saúde implantou sua aplicação web em instâncias de contêiner do Amazon Elastic Container Service (Amazon ECS) executadas por trás de um Application Load Balancer. O site fica lento quando o tráfego aumenta e a disponibilidade também diminui. A equipe de desenvolvimento configurou alarmes do Amazon CloudWatch para receber notificações sempre que houver uma restrição de disponibilidade, para que a equipe possa escalar os recursos. A empresa deseja uma solução automatizada para responder a esses eventos.

Qual das seguintes opções aborda o caso de uso fornecido?

**R: Configurar o AWS Auto Scaling para dimensionar o cluster do Amazon ECS quando a utilização da CPU do serviço ECS ultrapassar um limite**

**Opção correta:**

**Configurar o AWS Auto Scaling para dimensionar o cluster do Amazon ECS quando a utilização da CPU do serviço ECS ultrapassar um limite**

Use o assistente de primeira execução do Amazon ECS para criar um cluster e um serviço executado por trás de um balanceador de carga do Elastic Load Balancing. Em seguida, você pode configurar uma política de dimensionamento com monitoramento de destino que dimensiona seu serviço automaticamente com base na carga atual do aplicativo, medida pela utilização da CPU do serviço (das categorias ECS, ClusterName e ServiceName no CloudWatch).

Quando a utilização média da CPU do seu serviço ultrapassa 75% (ou seja, mais de 75% da CPU reservada para o serviço está sendo utilizada), um alarme de escalonamento horizontal aciona o Dimensionamento Automático do Serviço para adicionar outra tarefa ao seu serviço a fim de auxiliar no aumento da carga. Por outro lado, quando a utilização média da CPU do seu serviço cai abaixo da meta de utilização por um período prolongado, um alarme de escalonamento horizontal aciona uma redução na contagem desejada do serviço para liberar esses recursos do cluster para outras tarefas e serviços.

#### **Pergunta 15**

A equipe de análise de negócios de uma empresa executa consultas ad hoc nos serviços Oracle e PostgreSQL no Amazon RDS para preparar relatórios diários para a alta gerência. Para facilitar os relatórios de análise de negócios, a equipe de engenharia agora deseja replicar continuamente esses dados e consolidar esses bancos de dados em um data warehouse com escala de petabytes, transmitindo os dados para o Amazon Redshift.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução MAIS eficiente em termos de recursos e que exige a MENOR quantidade de tempo de desenvolvimento sem a necessidade de gerenciar a infraestrutura subjacente?

**R: Use o AWS Database Migration Service (AWS DMS) para replicar os dados dos bancos de dados no Amazon Redshift**

**Opção correta:**

**Use o AWS Database Migration Service (AWS DMS) para replicar os dados dos bancos de dados no Amazon Redshift**

O AWS Database Migration Service ajuda você a migrar bancos de dados para a AWS de forma rápida e segura. O banco de dados de origem permanece totalmente operacional durante a migração, minimizando o tempo de inatividade dos aplicativos que dependem dele. Com o AWS Database Migration Service, você pode replicar seus dados continuamente com alta disponibilidade e consolidar bancos de dados em um data warehouse em escala de petabytes, transmitindo dados para o Amazon Redshift e o Amazon S3.



Você pode migrar dados para bancos de dados do Amazon Redshift usando o AWS Database Migration Service. O Amazon Redshift é um serviço de data warehouse totalmente gerenciado e em escala de petabytes na nuvem. Com um banco de dados do Amazon Redshift como destino, você pode migrar dados de todos os outros bancos de dados de origem suportados.

O cluster do Amazon Redshift deve estar na mesma conta da AWS e na mesma região da AWS que a instância de replicação. Durante uma migração de banco de dados para o Amazon Redshift, o AWS DMS primeiro move os dados para um bucket do Amazon S3. Quando os arquivos residem em um bucket do Amazon S3, o AWS DMS os transfere para as tabelas adequadas no data warehouse do Amazon Redshift. O AWS DMS cria o bucket do S3 na mesma região da AWS que o banco de dados do Amazon Redshift. A instância de replicação do AWS DMS deve estar localizada na mesma região.

#### **Pergunta 16**

Uma startup migrou recentemente sua aplicação web monolítica para a Nuvem AWS. A aplicação é executada em uma única instância do Amazon EC2. Atualmente, a base de usuários é pequena e a startup não deseja investir esforços em estratégias elaboradas de recuperação de desastres ou no Auto Scaling Group. A aplicação pode ter um tempo de inatividade máximo de 10 minutos.

Em caso de falha, qual destas opções você sugeriria como um procedimento de recuperação automático e econômico para a instância?

**R: Configure um alarme do Amazon CloudWatch que acione a recuperação da instância do Amazon EC2, caso ela falhe. A instância, no entanto, só deve ser configurada com um volume do Amazon EBS.**

**Opção correta:**

**Configure um alarme do Amazon CloudWatch que acione a recuperação da instância do Amazon EC2, caso ela falhe. A instância, no entanto, só deve ser configurada com um volume do Amazon EBS.**

Se a sua instância falhar na verificação de status do sistema, você poderá usar as ações de alarme do Amazon CloudWatch para recuperá-la automaticamente. A opção de recuperação está disponível para mais de 90% das instâncias do Amazon EC2 implantadas. A opção de recuperação do Amazon CloudWatch funciona apenas para falhas na verificação do sistema, não para falhas na verificação de status da instância. Além disso, se você encerrar sua instância, ela não poderá ser recuperada.

Você pode criar um alarme do Amazon CloudWatch que monitora uma instância do Amazon EC2 e a recupera automaticamente caso ela seja prejudicada devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para reparo. Instâncias encerradas não podem ser recuperadas. Uma instância recuperada é idêntica à instância original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados da instância. Se a instância prejudicada estiver em um grupo de posicionamento, a instância recuperada será executada nesse grupo.

O processo de recuperação automática tenta recuperar sua instância para até três falhas distintas por dia. Sua instância poderá ser desativada posteriormente se a recuperação automática falhar e uma degradação de hardware for determinada como a causa raiz da falha original na verificação de status do sistema.

#### **Pergunta 17**

A equipe de engenharia de uma empresa está migrando o conteúdo estático do site de logística da empresa, hospedado em instâncias do Amazon EC2, para um bucket do Amazon S3. A equipe deseja usar uma distribuição do Amazon CloudFront para entregar o conteúdo estático. O grupo de segurança usado pelas instâncias do Amazon EC2 permite que o site seja acessado por um conjunto limitado de intervalos de IP dos fornecedores da empresa. Após a migração para o Amazon CloudFront, o acesso ao conteúdo estático deverá ser permitido apenas a partir dos endereços IP mencionados.

Quais opções você combinaria para criar uma solução que atendesse a esses requisitos? (Selecione duas)

**R: Configure uma identidade de acesso de origem (OAI) e associe-a à distribuição do Amazon CloudFront. Configure as permissões na política de bucket do Amazon S3 para que somente a OAI possa ler os objetos.**

**R: Crie uma ACL do AWS WAF e use uma condição de correspondência de IP para permitir tráfego apenas dos IPs permitidos no grupo de segurança do Amazon EC2. Associe esta nova ACL do AWS WAF à distribuição do Amazon CloudFront.**

**Opções corretas:**

- **Configure uma identidade de acesso de origem (OAI) e associe-a à distribuição do Amazon CloudFront. Configure as permissões na política de bucket do Amazon S3 para que somente a OAI possa ler os objetos.**

Ao usar o Amazon CloudFront com um bucket do Amazon S3 como origem, você pode configurar o Amazon CloudFront e o Amazon S3 de uma forma que forneça os seguintes benefícios:

Restringe o acesso ao bucket do Amazon S3 para que ele não seja acessível publicamente

Garante que os visualizadores (usuários) possam acessar o conteúdo no bucket somente por meio da distribuição especificada do Amazon CloudFront, ou seja, impede que eles acessem o conteúdo diretamente do bucket ou por meio de uma distribuição não intencional do CloudFront.

Para isso, configure o Amazon CloudFront para enviar solicitações autenticadas ao Amazon S3 e configure o Amazon S3 para permitir acesso apenas a solicitações autenticadas do Amazon CloudFront. O Amazon CloudFront oferece duas maneiras de enviar solicitações autenticadas a uma origem do Amazon S3: controle de acesso à origem (OAC) e identidade de acesso à origem (OAI).

#### **Alerta de exame:**

Observe que a AWS recomenda o uso do OAC porque ele oferece suporte a:

Todos os buckets do Amazon S3 em todas as regiões da AWS, incluindo regiões opt-in lançadas após dezembro de 2022

Criptografia do lado do servidor Amazon S3 com AWS KMS (SSE-KMS) Solicitações dinâmicas (POST, PUT, etc.) para Amazon S3

O OAI não funciona para os cenários da lista anterior ou requer soluções alternativas adicionais nesses cenários. No entanto, você continuará a ver respostas listando o OAI como a opção preferencial no exame real, pois leva cerca de 6 meses/1 ano para que um novo recurso apareça no exame.

- **Crie uma ACL do AWS WAF e use uma condição de correspondência de IP para permitir tráfego apenas dos IPs permitidos no grupo de segurança do Amazon EC2. Associe esta nova ACL do AWS WAF à distribuição do Amazon CloudFront.**

O AWS WAF é um firewall para aplicações web que permite monitorar as solicitações HTTP e HTTPS encaminhadas para os recursos protegidos da sua aplicação web. Você pode proteger os seguintes tipos de recursos:

- Distribuição do Amazon CloudFront
- API REST do Amazon API Gateway
- Balanceador de carga de aplicativo
- API GraphQL do AWS AppSync
- Grupo de usuários do Amazon Cognito

O AWS WAF também permite controlar o acesso ao seu conteúdo. Com base nas condições especificadas, como os endereços IP de origem das solicitações ou os valores das strings de consulta, seu recurso protegido responde às solicitações com o conteúdo solicitado, com um código de status HTTP 403 (Proibido) ou com uma resposta personalizada.

Se você quiser permitir ou bloquear solicitações da web com base nos endereços IP de origem das solicitações, crie uma ou mais condições de correspondência de IP por meio do seu AWS WAF. Uma condição de correspondência de IP lista até 10.000 endereços IP ou

intervalos de endereços IP de origem das suas solicitações.

Para o caso de uso fornecido, você deve adicionar os endereços IP permitidos no grupo de segurança do Amazon EC2 na condição de correspondência de IP.

#### **Pergunta 18**

Uma empresa de análise de big data está trabalhando em uma solução de rastreamento de veículos em tempo real. O fluxo de trabalho de processamento de dados envolve cargas de trabalho de banco de dados com uso intensivo de E/S e throughput. A equipe de desenvolvimento precisa armazenar esses dados em tempo real em um banco de dados NoSQL hospedado em uma instância do Amazon EC2 e precisa suportar até 25.000 IOPS por volume.

**Como arquiteto de soluções, qual dos seguintes tipos de volume do Amazon Elastic Block Store (Amazon EBS) você recomendaria para este caso de uso?**

**R: SSD IOPS provisionado (io1)**

**Opção correta:**

#### **SSD IOPS provisionado (io1)**

O SSD com IOPS Provisionado (io1) é apoiado por unidades de estado sólido (SSDs) e é uma opção de armazenamento de alto desempenho do Amazon EBS projetada para cargas de trabalho críticas de banco de dados e aplicativos com uso intensivo de E/S, bem como cargas de trabalho de banco de dados com alto throughput. O io1 foi projetado para fornecer um desempenho básico consistente de até 50 IOPS/GB a um máximo de 64.000 IOPS e fornecer até 1.000 MB/s de throughput por volume. Portanto, o tipo de volume io1 seria capaz de atender ao requisito de 25.000 IOPS por volume para o caso de uso em questão.

#### **Pergunta 19**

Um engenheiro de DevOps de uma empresa de TI acaba de atualizar uma instância do Amazon EC2 de t2.nano (0,5 GB de RAM, 1 vCPU) para u-12tb1.metal (12,3 TB de RAM, 448 vCPUs). **Como você classificaria essa atualização?**

**R: Este é um exemplo de escalabilidade vertical**

**Opção correta:**

#### **Este é um exemplo de escalabilidade vertical**

Escalabilidade vertical significa aumentar o tamanho da instância. Por exemplo, seu aplicativo é executado em um t2.micro. Escalar esse aplicativo verticalmente significa executá-lo em uma instância maior, como t2.large. Reduzir esse aplicativo verticalmente significa executá-lo em uma instância menor, como t2.nano. A escalabilidade é muito comum em sistemas não distribuídos, como um banco de dados. Geralmente, há um limite para o quanto você pode escalar verticalmente (limite de hardware). Nesse caso, como o tipo de instância foi atualizado de t2.nano para u-12tb1.metal, este é um exemplo de escalabilidade vertical.

#### **Pergunta 20**

A equipe de desenvolvimento de uma empresa de varejo quer otimizar o custo das instâncias do Amazon EC2. A equipe quer mover determinados trabalhos em lote noturnos para instâncias spot. A equipe contratou você como arquiteto de soluções para fornecer a orientação inicial.

**Qual das seguintes opções você identificaria como CORRETA em relação aos recursos das instâncias spot? (Selecione três)**

**R: Se uma solicitação spot for persistente, ela será aberta novamente após a interrupção da sua instância spot.**

**R: As frotas Spot podem manter a capacidade alvo iniciando instâncias de substituição após o término das instâncias Spot na frota**

**R: Quando você cancela uma solicitação de spot ativo, isso não encerra a instância associada**

**Opções corretas:**

- **Se uma solicitação spot for persistente, ela será aberta novamente após a interrupção da sua instância spot.**
  - Uma Instância Spot é uma instância não utilizada do Amazon EC2 que está disponível por um preço inferior ao preço sob demanda. Como as Instâncias Spot permitem que você solicite instâncias não utilizadas do Amazon EC2 com grandes descontos, você pode reduzir significativamente seus custos com o Amazon EC2. O preço por hora de uma Instância Spot é chamado de preço Spot. O preço Spot de cada tipo de instância em cada Zona de Disponibilidade é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e demanda de longo prazo por Instâncias Spot.
  - Uma solicitação de Instância Spot pode ser única ou persistente. Se a solicitação for persistente, ela será aberta novamente após a interrupção da sua Instância Spot. Se a solicitação for persistente e você interromper a sua Instância Spot, ela só será aberta após você iniciá-la.
- **As frotas Spot podem manter a capacidade alvo iniciando instâncias de substituição após o término das instâncias Spot na frota**
  - Uma Frota Spot é um conjunto de Instâncias Spot e, opcionalmente, Instâncias On-Demand, que é iniciado com base em critérios especificados por você. A Frota Spot seleciona os pools de capacidade Spot que atendem às suas necessidades e inicia Instâncias Spot para atingir a capacidade desejada para a frota. Por padrão, as Frotas Spot são configuradas para manter a capacidade desejada iniciando instâncias de substituição após o encerramento das Instâncias Spot na frota. Você pode enviar uma Frota Spot como uma solicitação única, que não persiste após o encerramento das instâncias. Você pode incluir solicitações de Instância On-Demand em uma solicitação de Frota Spot.
- **Quando você cancela uma solicitação de spot ativo, isso não encerra a instância associada**
  - Se a sua solicitação de Instância Spot estiver ativa e tiver uma Instância Spot em execução associada, ou se a sua solicitação de Instância Spot estiver desabilitada e tiver uma Instância Spot interrompida associada, o cancelamento da solicitação não encerra a instância; você deve encerrar a Instância Spot em execução manualmente. Além disso, para cancelar uma solicitação Spot persistente e encerrar suas Instâncias Spot, você deve cancelar a solicitação Spot primeiro e, em seguida, encerrar as Instâncias Spot.

## **Pergunta 21**

A equipe de DevOps de uma empresa de TI criou uma VPC personalizada (V1) e conectou um Gateway de Internet (I1) a ela. A equipe também criou uma sub-rede (S1) nessa VPC personalizada e adicionou uma rota à tabela de rotas dessa sub-rede (R1), que direciona o tráfego da Internet para o Gateway de Internet. Agora, a equipe inicia uma instância do Amazon EC2 (E1) na sub-rede S1 e atribui um endereço IPv4 público a essa instância. Em seguida, a equipe também inicia uma instância de Tradução de Endereços de Rede (NAT) (N1) na sub-rede S1.

Na configuração de infraestrutura fornecida, qual das seguintes entidades está realizando a tradução de endereços de rede para a instância E1 do Amazon EC2?

**R: Gateway de Internet (I1)**

**Opção correta:**

### **Gateway de Internet (I1)**

Um Gateway de Internet é um componente de VPC escalonado horizontalmente, redundante e altamente disponível que permite a comunicação entre sua VPC e a Internet.

Um Gateway de Internet tem duas finalidades: fornecer um destino nas suas tabelas de rotas de VPC para tráfego roteável pela Internet e realizar a tradução de endereços de rede (NAT) para instâncias que receberam endereços IPv4 públicos. Portanto, para a instância E1, a Tradução de Endereços de Rede é realizada pelo Gateway de Internet I1. Além disso, um Gateway de Internet suporta tráfego IPv4 e IPv6. Ele não causa riscos de disponibilidade ou restrições de largura de banda no tráfego da sua rede.

Para habilitar o acesso de ou para a Internet para instâncias em uma sub-rede em uma VPC, você deve fazer o seguinte:

Anexe um gateway de Internet à sua VPC.

Adicione uma rota à tabela de rotas da sua sub-rede que direcione o tráfego da Internet para o gateway de Internet. Se uma sub-rede estiver associada a uma tabela de rotas que tenha uma rota para um gateway de Internet, ela será chamada de sub-rede pública. Se uma sub-rede estiver associada a uma tabela de rotas que não tenha uma rota para um gateway de Internet, ela será chamada de sub-rede privada.

Certifique-se de que as instâncias na sua sub-rede tenham um endereço IP globalmente exclusivo (endereço IPv4 público, endereço IP elástico ou endereço IPv6).

Certifique-se de que suas listas de controle de acesso à rede e regras de grupo de segurança permitam que o tráfego relevante flua de e para sua instância.

## **Pergunta 22**

Uma empresa líder em agregação de notícias oferece centenas de produtos e serviços digitais para clientes que vão de escritórios de advocacia a bancos e consumidores. A empresa cobra seus clientes com base em dados de fluxo de cliques por unidade fornecidos aos clientes. Como a empresa opera em um setor regulamentado, ela precisa ter os mesmos dados de fluxo de cliques ordenados disponíveis para auditoria em uma janela de 7 dias.

Como arquiteto de soluções, qual dos seguintes serviços da AWS oferece a capacidade de executar o processo de cobrança e o processo de auditoria nos dados de fluxo de cliques fornecidos na mesma ordem?

**R: Fluxos de dados do Amazon Kinesis**

**Opção correta:**

**Fluxos de dados do Amazon Kinesis**

O Amazon Kinesis Data Streams (KDS) é um serviço de streaming de dados em tempo real altamente escalável e durável. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de bancos de dados, transações financeiras, feeds de mídias sociais, registros de TI e eventos de rastreamento de localização. Os dados coletados ficam disponíveis em milissegundos para permitir casos de uso de análise em tempo real, como painéis em tempo real, detecção de anomalias em tempo real, precificação dinâmica e muito mais.

O Amazon Kinesis Data Streams permite o processamento em tempo real de big data em streaming. Ele permite a ordenação de registros, bem como a capacidade de ler e/ou reproduzir registros na mesma ordem para vários aplicativos do Amazon Kinesis. A Biblioteca de Cliente do Amazon Kinesis (KCL) entrega todos os registros de uma determinada chave de partição para o mesmo processador de registros, facilitando a criação de vários aplicativos que leem o mesmo fluxo de dados do Amazon Kinesis (por exemplo, para realizar contagem, agregação e filtragem). O Amazon Kinesis Data Streams é recomendado quando você precisa consumir registros na mesma ordem algumas horas depois.

Por exemplo, você tem um aplicativo de cobrança e um aplicativo de auditoria que rodam algumas horas atrás do aplicativo de cobrança. Como o Amazon Kinesis Data Streams armazena dados por no máximo

365 dias, você pode facilmente executar o aplicativo de auditoria até 7 dias atrás do aplicativo de cobrança.

## **Pergunta 23**

A equipe de manutenção de aplicativos de uma empresa notou que o aplicativo de produção fica muito lento quando os relatórios de negócios são executados no banco de dados Amazon RDS. Esses relatórios buscam uma grande quantidade de dados e têm consultas complexas com múltiplas junções, abrangendo diversas tabelas principais

críticas para os negócios. As métricas de CPU, memória e armazenamento representam cerca de 50% da capacidade total.

Você pode recomendar uma maneira melhorada e econômica de gerar relatórios comerciais sem afetar o aplicativo de produção?

**R: Crie uma réplica de leitura e conecte a ferramenta/aplicativo de geração de relatórios a ela**

**Opção correta:**

**Crie uma réplica de leitura e conecte a ferramenta/aplicativo de geração de relatórios a ela**

As Réplicas de Leitura do Amazon RDS oferecem desempenho e durabilidade aprimorados para instâncias de banco de dados (BD) do Amazon RDS. Elas facilitam o dimensionamento horizontal elástico, além das restrições de capacidade de uma única instância de banco de dados, para cargas de trabalho de banco de dados com alto consumo de leitura. Você pode criar uma ou mais réplicas de uma determinada Instância de Banco de Dados de origem e atender a um alto volume de tráfego de leitura de aplicativos a partir de várias cópias dos seus dados, aumentando assim a taxa de transferência agregada de leitura. As réplicas de leitura também podem ser promovidas, quando necessário, para se tornarem instâncias de banco de dados autônomas.

Há diversos cenários em que a implantação de uma ou mais réplicas de leitura para uma determinada instância de banco de dados de origem pode fazer sentido. Motivos comuns para a implantação de uma réplica de leitura incluem:

1. Escalabilidade além da capacidade de computação ou E/S de uma única instância de banco de dados para cargas de trabalho de banco de dados com alto consumo de leitura. Esse excesso de tráfego de leitura pode ser direcionado para uma ou mais réplicas de leitura.
2. Atendendo tráfego de leitura enquanto a instância do banco de dados de origem estiver indisponível. Se a sua instância do banco de dados de origem não puder receber solicitações de E/S (por exemplo, devido à suspensão de E/S para backups ou manutenção programada), você pode direcionar o tráfego de leitura para sua(s) réplica(s) de leitura. Para este caso de uso, lembre-se de que os dados na réplica de leitura podem estar "obsoletos", pois a instância do banco de dados de origem está indisponível.
3. Cenários de relatórios comerciais ou de armazenamento de dados; talvez você queira que as consultas de relatórios comerciais sejam executadas em uma réplica de leitura, em vez de na sua instância de banco de dados de produção principal.
4. Você pode usar uma réplica de leitura para recuperação de desastres da instância do banco de dados de origem, na mesma região da AWS ou em outra região.

#### **Pergunta 24**

Uma empresa de varejo conectou seu data center local à Nuvem AWS por meio do AWS Direct Connect. A empresa deseja resolver consultas de DNS (Sistema de Nomes de Domínio) para quaisquer recursos na rede local a partir da VPC da AWS e também resolver quaisquer consultas de DNS para recursos na VPC da AWS a partir da rede local.

Como arquiteto de soluções, quais das seguintes soluções podem ser combinadas para abordar o caso de uso fornecido? (Selecione duas)

**R: Crie um ponto de extremidade de saída no Amazon Route 53 Resolver e, em seguida, o Amazon Route 53 Resolver poderá encaminhar condicionalmente consultas para resolvedores na rede local por meio desse ponto de extremidade**

**R: Crie um ponto de extremidade de entrada no Amazon Route 53 Resolver e, em seguida, os resolvedores de DNS na rede local podem encaminhar consultas de DNS para o Amazon Route 53 Resolver por meio desse ponto de extremidade**

**Opções corretas:**

- Crie um ponto de extremidade de entrada no Amazon Route 53 Resolver e, em seguida, os resolvedores de DNS na rede local podem encaminhar consultas de DNS para o Amazon Route 53 Resolver por meio desse ponto de extremidade
- Crie um ponto de extremidade de saída no Amazon Route 53 Resolver e, em seguida, o Amazon Route 53 Resolver poderá encaminhar condicionalmente consultas para resolvedores na rede local por meio desse ponto de extremidade

→ O Amazon Route 53 é um serviço web de Sistema de Nomes de Domínio (DNS) em nuvem altamente disponível e escalável. O Amazon Route 53 conecta efetivamente as solicitações dos usuários à infraestrutura em execução na AWS – como instâncias do Amazon EC2 – e também pode ser usado para rotear usuários para infraestruturas fora da AWS. Por padrão, o Amazon Route 53 Resolver responde automaticamente às consultas DNS para nomes de domínio VPC locais para instâncias do Amazon EC2. Você pode integrar a resolução de DNS entre o Resolver e os resolvedores de DNS em sua rede local configurando regras de encaminhamento.

Para resolver quaisquer consultas de DNS para recursos na AWS VPC da rede local, você pode criar um endpoint de entrada no Amazon Route 53 Resolver e, então, os resolvedores de DNS na rede local podem encaminhar consultas de DNS para o Amazon Route 53 Resolver por meio desse endpoint.

Para resolver consultas DNS para quaisquer recursos na rede local a partir da VPC da AWS, você pode criar um endpoint de saída no Amazon Route 53 Resolver, que poderá encaminhar consultas condicionalmente para resolvedores na rede local por meio desse endpoint. Para encaminhar consultas condicionalmente, você precisa criar regras do Resolver que especifiquem os nomes de domínio das consultas DNS que você deseja encaminhar (como example.com) e os endereços IP dos resolvedores DNS na rede local para os quais você deseja encaminhar as consultas.

#### **Pergunta 25**

Qual dos seguintes serviços da AWS fornece uma solução altamente disponível e tolerante a falhas para capturar eventos de fluxo de cliques da origem e, em seguida, fornecer um feed simultâneo do fluxo de dados para os aplicativos downstream?

**R: Fluxos de dados do Amazon Kinesis**

**Opção correta:**

#### **Fluxos de dados do Amazon Kinesis**

O Amazon Kinesis Data Streams (KDS) é um serviço de streaming de dados em tempo real altamente escalável e durável. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de bancos de dados, transações financeiras, feeds de mídias sociais, registros de TI e eventos de rastreamento de localização. Os dados coletados ficam disponíveis em milissegundos para permitir casos de uso de análise em tempo real, como painéis em tempo real, detecção de anomalias em tempo real, precificação dinâmica e muito mais.

O Amazon Kinesis Data Streams permite o processamento em tempo real de big data de streaming. Ele fornece ordenação de registros, bem como a capacidade de ler e/ou reproduzir registros na mesma ordem para vários aplicativos do Amazon Kinesis. A Amazon Kinesis Client Library (KCL) entrega todos os registros para uma determinada chave de partição para o mesmo processador de registro, facilitando a criação de vários aplicativos lendo do mesmo fluxo de dados do Amazon Kinesis (por exemplo, para executar contagem, agregação e filtragem).

O Amazon Kinesis Data Streams é recomendado quando você precisa que vários aplicativos consumam o mesmo fluxo simultaneamente. Por exemplo, você tem um aplicativo que atualiza um painel em tempo real e outro que arquiva dados no Amazon Redshift. Você deseja que ambos os aplicativos consumam dados do mesmo fluxo simultaneamente e de forma independente.

#### **Alerta de exame:**

Lembre-se de que o Amazon Kinesis Data Firehose é usado para carregar dados de streaming em armazenamentos de dados (Amazon S3, Amazon Redshift, Amazon Elasticsearch Service e Splunk), enquanto o Kinesis Data Streams oferece suporte para

processamento de dados de streaming em tempo real. Ele permite a ordenação de registros, bem como a capacidade de ler e/ou reproduzir registros na mesma ordem para vários aplicativos Amazon Kinesis downstream.

#### **Pergunta 26**

Uma empresa de jogos utiliza Application Load Balancers em instâncias do Amazon EC2 para diferentes serviços e microsserviços. A arquitetura se tornou complexa com o excesso de Application Load Balancers em diversas regiões da AWS. Atualizações de segurança, configurações de firewall e lógica de roteamento de tráfego se tornaram complexas com o excesso de endereços IP e configurações.

A empresa está buscando uma maneira fácil e eficaz de reduzir o número de endereços IP permitidos pelo firewall e gerenciar facilmente toda a infraestrutura de rede. Qual destas opções representa uma solução adequada para essa necessidade?

**R: Inicie o AWS Global Accelerator e crie endpoints para todas as regiões. Registre os Application Load Balancers de cada região nos endpoints correspondentes.**

**Opção correta:**

**Inicie o AWS Global Accelerator e crie endpoints para todas as regiões. Registre os Application Load Balancers de cada região nos endpoints correspondentes.**

O AWS Global Accelerator é um serviço de rede que envia o tráfego dos seus usuários pela infraestrutura de rede global da Amazon Web Service, melhorando o desempenho dos seus usuários de internet em até 60%. Quando a internet está congestionada, as otimizações automáticas de roteamento do Global Accelerator ajudam a manter a perda de pacotes, o jitter e a latência consistentemente baixos.

Com o AWS Global Accelerator, você recebe dois IPs estáticos globais voltados para o cliente para simplificar o gerenciamento de tráfego. No back-end, adicione ou remova suas origens de aplicativos da AWS, como balanceadores de carga de rede, balanceadores de carga de aplicativos, endereço IP elástico (EIP) e instâncias do Amazon EC2, sem fazer alterações no usuário. Para mitigar falhas de endpoint, o AWS Global Accelerator redireciona automaticamente seu tráfego para o endpoint saudável disponível mais próximo.

#### **Pergunta 27**

Um aplicativo de assistência médica processa os dados de saúde em tempo real dos pacientes em um fluxo de trabalho analítico. Com um aumento acentuado no número de usuários, o sistema se tornou lento e, às vezes, até mesmo sem resposta, pois não tem um mecanismo de repetição. A startup está buscando uma solução escalável que tenha sobrecarga mínima de implementação.

Qual das opções a seguir você recomendaria como alternativa escalável à solução atual?

**R: Use o Amazon Kinesis Data Streams para ingerir os dados, processá-los usando o AWS Lambda ou executar análises usando o Amazon Kinesis Data Analytics**

**Opção correta:**

**Use o Amazon Kinesis Data Streams para ingerir os dados, processá-los usando o AWS Lambda ou executar análises usando o Amazon Kinesis Data Analytics**

O Amazon Kinesis Data Streams (KDS) é um serviço de streaming de dados em tempo real massivamente escalável e durável com suporte para mecanismo de repetição. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de banco de dados, transações financeiras, feeds de mídia social, logs de TI e eventos de rastreamento de localização. Os dados coletados ficam disponíveis em milissegundos para permitir casos de uso de análise em tempo real, como painéis em tempo real, detecção de anomalias em tempo real, preços dinâmicos e muito mais.

O KDS garante que seus dados de streaming estejam disponíveis para vários aplicativos de análise em tempo real, para o Amazon S3 ou AWS Lambda dentro de 70 milissegundos dos dados coletados. Os fluxos de dados do Amazon Kinesis escalam de megabytes para terabytes por hora e escalam de milhares para milhões de registros PUT



por segundo. Você pode ajustar dinamicamente a taxa de transferência do seu fluxo a qualquer momento com base no volume dos seus dados de entrada.

#### **Pergunta 28**

Uma empresa líder em jogos online está migrando seu aplicativo principal para a Nuvem AWS para entregar seus jogos online a usuários em todo o mundo. A empresa gostaria de usar um Balanceador de Carga de Rede para processar milhões de solicitações por segundo. A equipe de engenharia provisionou várias instâncias em uma sub-rede pública e especificou esses IDs de instância como alvos para o NLB.

Como arquiteto de soluções, você pode ajudar a equipe de engenharia a entender o mecanismo de roteamento correto para essas instâncias de destino?

**R: O tráfego é roteado para instâncias usando o endereço IP privado primário especificado na interface de rede primária para a instância**

**Opção correta:**

**O tráfego é roteado para instâncias usando o endereço IP privado primário especificado na interface de rede primária para a instância**

Um balanceador de carga de rede funciona na quarta camada do modelo de Interconexão de Sistemas Abertos (OSI). Ele pode processar milhões de solicitações por segundo. Após receber uma solicitação de conexão, o balanceador de carga seleciona um destino do grupo de destinos para a regra padrão. Ele tenta abrir uma conexão TCP com o destino selecionado na porta especificada na configuração do listener.

Roteamento de solicitações e endereços IP - Se você especificar destinos usando um ID de instância, o tráfego será roteado para as instâncias usando o endereço IP privado primário especificado na interface de rede primária da instância. O balanceador de carga reescreve o endereço IP de destino do pacote de dados antes de encaminhá-lo para a instância de destino.

Se você especificar destinos usando endereços IP, poderá rotear o tráfego para uma instância usando qualquer endereço IP privado de uma ou mais interfaces de rede. Isso permite que vários aplicativos em uma instância usem a mesma porta. Observe que cada interface de rede pode ter seu próprio grupo de segurança. O balanceador de carga reescreve o endereço IP de destino antes de encaminhá-lo ao destino.

#### **Pergunta 29**

Uma organização de varejo está migrando alguns de seus dados locais para a Nuvem AWS. A equipe de DevOps da organização configurou uma conexão VPN IPsec gerenciada pela AWS entre sua rede local remota e sua Amazon VPC pela internet.

Qual das opções a seguir representa a configuração correta para a conexão VPN IPsec?

**R: Crie um gateway privado virtual (VGW) no lado da AWS da VPN e um gateway do cliente no lado local da VPN**

**Opção correta:**

**Crie um gateway privado virtual (VGW) no lado da AWS da VPN e um gateway do cliente no lado local da VPN**

A Amazon VPC oferece a possibilidade de criar uma conexão VPN IPsec (também conhecida como VPN site a site da AWS) entre redes de clientes remotos e sua Amazon VPC pela internet. A seguir, os principais conceitos de uma VPN site a site:

Gateway privado virtual: um gateway privado virtual (VGW), também conhecido como gateway VPN, é o ponto de extremidade no lado do AWS VPC da sua conexão VPN.

Conexão VPN: uma conexão segura entre seu equipamento local e suas VPCs.

Túnel VPN: um link criptografado por onde os dados podem passar da rede do cliente para ou da AWS.

Gateway do cliente: um recurso da AWS que fornece informações à AWS sobre seu dispositivo Gateway do cliente.

Dispositivo de gateway do cliente: um dispositivo físico ou aplicativo de software no lado do cliente da conexão VPN de site para site.

### Pergunta 30

Uma empresa de biotecnologia possui diversos fluxos de trabalho de Computação de Alto Desempenho (HPC) que processam e analisam genomas de doenças hereditárias com rapidez e precisão. A empresa busca migrar esses fluxos de trabalho de sua infraestrutura local para a Nuvem AWS.

Como arquiteto de soluções, qual dos seguintes componentes de rede você recomendaria nas instâncias do Amazon EC2 que executam esses fluxos de trabalho de HPC?

**R: Adaptador de Tecido Elástico (EFA)**

**Opção correta:**

### Adaptador de Tecido Elástico (EFA)

Um Adaptador de Tecido Elástico (EFA) é um dispositivo de rede que você pode conectar à sua instância do Amazon EC2 para acelerar aplicações de Computação de Alto Desempenho (HPC) e aprendizado de máquina. Ele aprimora o desempenho da comunicação entre instâncias, essencial para o dimensionamento de aplicações de HPC e aprendizado de máquina. Os dispositivos EFA fornecem todas as funcionalidades dos dispositivos Adaptadores de Rede Elástica (ENA), além de uma nova interface de hardware de bypass do sistema operacional que permite que aplicações no espaço do usuário se comuniquem diretamente com a funcionalidade de transporte confiável fornecida pelo hardware.

### Pergunta 31

Uma empresa de serviços financeiros deseja migrar os clusters de servidores de arquivos Windows de seus data centers. Ela busca serviços de armazenamento em nuvem que ofereçam total compatibilidade com o Windows. Você consegue identificar os serviços de armazenamento da AWS que oferecem armazenamento de arquivos altamente confiável, acessível pelo protocolo SMB (Server Message Block), padrão do setor, compatível com sistemas Windows? (Selecione duas opções)

**R: Configuração do gateway de arquivos do AWS Storage Gateway R: Amazon FSx para servidor de arquivos do Windows**

**Opções corretas:**

- **Amazon FSx para servidor de arquivos do Windows**

O Amazon FSx para Windows File Server é um armazenamento de arquivos totalmente gerenciado e altamente confiável, acessível através do protocolo SMB (Server Message Block), padrão do setor. Ele é baseado no Windows Server e oferece uma ampla gama de recursos administrativos, como cotas de usuários, restauração de arquivos do usuário final e integração com o Microsoft Active Directory (AD).

- **Configuração do gateway de arquivos do AWS Storage Gateway**

Dependendo do caso de uso, o AWS Storage Gateway oferece três tipos de interfaces de armazenamento para aplicativos locais: Arquivo, Volume e Fita. O File Gateway permite armazenar e recuperar objetos no Amazon S3 usando protocolos de arquivo como Network File System (NFS) e Server Message Block (SMB).

### Pergunta 32

Um aplicativo legado é construído usando uma arquitetura monolítica fortemente acoplada. Devido ao aumento acentuado no número de usuários, o desempenho do aplicativo se degradou. A empresa agora deseja desacoplar a arquitetura e adotar a arquitetura de microsserviços da AWS. Alguns desses microsserviços precisam lidar com processos de execução rápida, enquanto outros precisam lidar com processos mais lentos. Qual dessas opções você identificaria como a maneira correta de conectar esses microsserviços?

**R: Configurar a fila do Amazon Simple Queue Service (Amazon SQS) para desacoplar os microserviços que executam processos mais rápidos dos microserviços que executam processos mais lentos**

**Opção correta:**

**Configurar a fila do Amazon Simple Queue Service (Amazon SQS) para desacoplar os microserviços que executam processos mais rápidos dos microserviços que executam processos mais lentos**

O Amazon Simple Queue Service (Amazon SQS) é um serviço de enfileiramento de mensagens totalmente gerenciado que permite desacoplar e escalar microserviços, sistemas distribuídos e aplicações sem servidor. O Amazon SQS elimina a complexidade e a sobrecarga associadas ao gerenciamento e operação de middleware orientado a mensagens e permite que os desenvolvedores se concentrem na diferenciação do trabalho. Usando o SQS, você pode enviar, armazenar e receber mensagens entre componentes de software em qualquer volume, sem perder mensagens ou exigir a disponibilidade de outros serviços.

Use o Amazon SQS para transmitir qualquer volume de dados, em qualquer nível de throughput, sem perder mensagens ou exigir a disponibilidade de outros serviços. O Amazon SQS permite desacoplar componentes de aplicativos para que sejam executados e falhem independentemente, aumentando a tolerância geral a falhas do sistema. Várias cópias de cada mensagem são armazenadas redundantemente em várias zonas de disponibilidade para que estejam disponíveis sempre que necessário. A capacidade de armazenar as mensagens e reproduzi-las é um recurso muito importante para desacoplar a arquitetura do sistema, conforme necessário no caso de uso atual.

### **Pergunta 33**

Uma empresa de comércio eletrônico está usando o Elastic Load Balancing (ELB) para sua frota de instâncias do Amazon EC2 distribuídas em duas Zonas de Disponibilidade (AZs), com uma instância como destino na Zona de Disponibilidade A e quatro instâncias como destino na Zona de Disponibilidade B. A empresa está fazendo benchmarking de desempenho do servidor quando o balanceamento de carga entre zonas está habilitado em comparação ao caso quando o balanceamento de carga entre zonas está desabilitado. Como arquiteto de soluções, qual dos seguintes resultados de distribuição de tráfego você identificaria como correto?

**R: Com o balanceamento de carga entre zonas habilitado, uma instância na Zona de Disponibilidade A recebe 20% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 20% do tráfego cada. Com o balanceamento de carga entre zonas desabilitado, uma instância na Zona de Disponibilidade A recebe 50% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 12,5% do tráfego cada.**

**Opção correta:**

**Com o balanceamento de carga entre zonas habilitado, uma instância na Zona de Disponibilidade A recebe 20% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 20% do tráfego cada. Com o balanceamento de carga entre zonas desabilitado, uma instância na Zona de Disponibilidade A recebe 50% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 12,5% do tráfego cada.**

Os nós do seu balanceador de carga distribuem solicitações de clientes para destinos registrados. Quando o balanceamento de carga entre zonas está habilitado, cada nó do balanceador de carga distribui o tráfego entre os destinos registrados em todas as Zonas de Disponibilidade habilitadas. Portanto, uma instância na Zona de Disponibilidade A recebe 20% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 20% do tráfego cada. Quando o balanceamento de carga entre zonas está desabilitado, cada nó do balanceador de carga distribui o tráfego apenas entre os destinos registrados em sua Zona de Disponibilidade. Portanto, uma instância na Zona de Disponibilidade A recebe 50% do tráfego e quatro instâncias na Zona de Disponibilidade B recebem 12,5% do tráfego cada.

Considere os diagramas a seguir (o cenário ilustrado nos diagramas envolve 10 instâncias de destino divididas em 2 AZs) para entender o efeito do balanceamento de carga entre zonas.

Se o balanceamento de carga entre zonas estiver habilitado, cada um dos 10 destinos receberá 10% do tráfego. Isso ocorre porque cada nó do balanceador de

carga pode rotear 50% do tráfego do cliente para todos os 10 destinos. Se o balanceamento de carga entre zonas estiver desabilitado:

Cada um dos dois alvos na Zona de Disponibilidade A recebe 25% do tráfego.

Cada um dos oito alvos na Zona de Disponibilidade B recebe 6,25% do tráfego.

Isso ocorre porque cada nó do balanceador de carga pode rotear 50% do tráfego do cliente apenas para destinos em sua Zona de Disponibilidade

#### **Pergunta 34**

Uma empresa de análise de dados gerencia um aplicativo que armazena dados do usuário em uma tabela do Amazon DynamoDB. A equipe de desenvolvimento observou que, ocasionalmente, o aplicativo grava dados corrompidos na tabela do Amazon DynamoDB. Assim que o problema é detectado, a equipe precisa remover os dados corrompidos o mais rápido possível.

O que você recomenda?

**R: Use a recuperação de ponto no tempo do Amazon DynamoDB para restaurar a tabela ao estado imediatamente anterior à gravação dos dados corrompidos**

**Opção correta:**

**Use a recuperação de ponto no tempo do Amazon DynamoDB para restaurar a tabela ao estado imediatamente anterior à gravação dos dados corrompidos**

O Amazon DynamoDB permite que você faça backup dos dados da sua tabela continuamente usando a recuperação point-in-time (PITR). Ao habilitar a PITR, o DynamoDB faz backup dos dados da sua tabela automaticamente com granularidade por segundo, para que você possa restaurar para qualquer segundo nos 35 dias anteriores.

O PITR ajuda a proteger você contra gravações e exclusões acidentais. Por exemplo, se um script de teste gravar acidentalmente em uma tabela de produção do DynamoDB ou alguém emitir uma chamada "DeleteItem" por engano, o PITR está aqui para ajudar.

#### **Pergunta 35**

Uma startup criou uma nova aplicação web para que os usuários respondam a uma pesquisa de avaliação de risco para sintomas de COVID-19 por meio de um questionário autoaplicável. A startup adquiriu o domínio covid19survey.com usando o Amazon Route 53. A equipe de desenvolvimento web gostaria de criar um registro no Amazon Route 53 para que todo o tráfego para covid19survey.com seja roteado para www.covid19survey.com.

Como arquiteto de soluções, qual das seguintes opções é a solução MAIS econômica que você recomendaria à equipe de desenvolvimento web?

**R: Crie um registro de alias para covid19survey.com que direcione o tráfego para [www.covid19survey.com](http://www.covid19survey.com)**

**Opção correta:**

**Crie um registro de alias para covid19survey.com que direcione o tráfego para [www.covid19survey.com](http://www.covid19survey.com)**

Os registros de alias fornecem uma extensão específica do Amazon Route 53 para a funcionalidade de DNS. Os registros de alias permitem rotear tráfego para recursos selecionados da AWS, como distribuições do Amazon CloudFront e buckets do Amazon S3.

Você pode criar um registro de alias no nó superior de um namespace DNS, também conhecido como apex de zona. No entanto, não é possível criar um registro CNAME para o nó superior do namespace DNS. Portanto, se você registrar o nome DNS covid19survey.com, o apex de zona será covid19survey.com. Você não pode criar um registro CNAME para covid19survey.com, mas pode criar um registro de alias para covid19survey.com que roteie o tráfego para www.covid19survey.com.

#### **Alerta de exame:**

Observe também que o Amazon Route 53 não cobra por consultas de alias para recursos da

AWS, mas cobra por consultas CNAME. Além disso, um registro de alias só pode redirecionar consultas para recursos selecionados da AWS, como buckets do Amazon S3, distribuições do Amazon CloudFront e outro registro na mesma zona hospedada do Amazon Route 53; no entanto, um registro CNAME pode redirecionar consultas DNS para qualquer registro DNS. Portanto, você pode criar um registro CNAME que redireciona consultas de app.covid19survey.com para app.covid19survey.net.

#### **Pergunta 36**

Uma empresa de mídia tem sua sede corporativa em Los Angeles, com um data center local que utiliza uma conexão AWS Direct Connect com a AWS VPC. As filiais em São Francisco e Miami usam conexões VPN Site-to-Site da AWS para se conectar à AWS VPC. A empresa busca uma solução para que as filiais enviem e recebam dados entre si, bem como com a sede corporativa.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você recomendaria para esse caso de uso?

**R: AWS VPN CloudHub**

**Opção correta:**

**AWS VPN CloudHub**

Se você tiver várias conexões AWS Site-to-Site VPN, poderá fornecer comunicação segura entre sites usando o AWS VPN CloudHub. Isso permite que seus sites remotos se comuniquem entre si, e não apenas com a VPC. Sites que usam conexões AWS Direct Connect com o gateway privado virtual também podem fazer parte do AWS VPN CloudHub. O VPN CloudHub opera em um modelo hub-and-spoke simples que você pode usar com ou sem uma VPC. Este design é adequado se você tiver várias filiais e conexões de internet existentes e gostaria de implementar um modelo hub-and-spoke conveniente e potencialmente de baixo custo para conectividade primária ou de backup entre esses escritórios remotos.

Conforme o caso de uso fornecido, a sede corporativa tem uma conexão AWS Direct Connect com a VPC e as filiais têm conexões Site-to-Site VPN com a VPC. Portanto, usando o AWS VPN CloudHub, as filiais podem enviar e receber dados entre si, bem como com suas sedes corporativas.

#### **Pergunta 37**

Uma empresa de TI busca migrar sua infraestrutura local para a Nuvem AWS. A empresa possui um portfólio de aplicativos, alguns dos quais utilizam licenças vinculadas ao servidor, válidas para o ano seguinte. Para utilizar as licenças, o CTO deseja usar hosts dedicados por um ano e, posteriormente, migrar as instâncias fornecidas para a locação padrão.

Como arquiteto de soluções, qual das seguintes opções você identificaria como CORRETA para alterar a locação de uma instância depois de iniciá-la? (Selecione duas)

**R: Você pode alterar a locação de uma instância de dedicada para host**

**R: Você pode alterar a locação de uma instância de host para dedicada**

**Opções corretas:**

- **Você pode alterar a locação de uma instância de dedicada para host**
- **Você pode alterar a locação de uma instância de host para dedicada**

Cada instância do Amazon EC2 que você inicia em uma VPC tem um atributo de locação. Este atributo tem os seguintes valores.

instâncias do Amazon EC2 são executadas em uma base de locação compartilhada.

Instâncias Dedicadas são instâncias do Amazon EC2 executadas em uma nuvem privada virtual (VPC) em hardware dedicado a um único cliente. Instâncias Dedicadas que pertencem a diferentes contas da AWS são fisicamente isoladas no nível do hardware. No entanto, Instâncias Dedicadas podem compartilhar hardware com outras instâncias da mesma conta da AWS que não sejam Instâncias Dedicadas.

Um Host Dedicado também é um servidor físico dedicado ao seu uso. Com um Host

Dedicado, você tem visibilidade e controle sobre como as instâncias são alocadas no servidor.

### **Pergunta 38**

Uma organização da AWS utiliza Políticas de Controle de Serviço (SCPs) para controle centralizado sobre o máximo de permissões disponíveis para todas as contas em sua organização. Isso permite que a organização garanta que todas as contas permaneçam dentro das diretrizes de controle de acesso da organização.

Quais dos cenários fornecidos estão corretos em relação às permissões descritas abaixo? (Selecione três)

**R: A política de controle de serviço (SCP) afeta todos os usuários e funções nas contas de membro, incluindo o usuário raiz das contas de membro**

**R: Se um usuário ou função tiver uma política de permissão do IAM que conceda acesso a uma ação que não é permitida ou explicitamente negada pela política de controle de serviço (SCP) aplicável, o usuário ou a função não poderá executar essa ação.**

**R: A política de controle de serviço (SCP) não afeta a função vinculada ao serviço**

**Opções corretas:**

- **Se um usuário ou função tiver uma política de permissão do IAM que conceda acesso a uma ação que não é permitida ou explicitamente negada pela política de controle de serviço (SCP) aplicável, o usuário ou a função não poderá executar essa ação.**
- **A política de controle de serviço (SCP) afeta todos os usuários e funções nas contas de membro, incluindo o usuário raiz das contas de membro**
- **A política de controle de serviço (SCP) não afeta a função vinculada ao serviço**

A política de controle de serviço (SCP) é um tipo de política que pode ser usada para gerenciar sua organização. Ela oferece controle centralizado sobre as permissões máximas disponíveis para todas as contas da sua organização, permitindo que você garanta que suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização.

Na política de controle de serviço (SCP), você pode restringir quais serviços, recursos e ações de API individuais da AWS os usuários e funções em cada conta de membro podem acessar. Você também pode definir condições para quando restringir o acesso a serviços, recursos e ações de API da AWS. Essas restrições substituem até mesmo os administradores de contas de membro na organização.

Observe os seguintes efeitos nas permissões em relação à política de controle de serviço (SCP):

Se um usuário ou função tiver uma política de permissão do IAM que conceda acesso a uma ação que não é permitida ou explicitamente negada pela política de controle de serviço (SCP) aplicável, o usuário ou a função não poderá executar essa ação.

A política de controle de serviço (SCP) afeta todos os usuários e funções nas contas de membro, incluindo o usuário raiz das contas de membro.

A política de controle de serviço (SCP) não afeta nenhuma função vinculada ao serviço.

### **Pergunta 39**

Uma empresa deseja aprimorar seu aplicativo de jogos adicionando uma tabela de classificação que utiliza um algoritmo proprietário complexo baseado nas métricas de desempenho dos usuários participantes para identificar os melhores usuários em tempo real. Os requisitos técnicos exigem alta elasticidade, baixa latência e processamento em tempo real para fornecer dados de usuários personalizáveis para a comunidade. A tabela de classificação seria acessada por milhões de usuários simultaneamente.

Qual das seguintes opções dá suporte ao caso de uso do Amazon ElastiCache para atender aos requisitos fornecidos? (Selecione duas)

**R: Use o Amazon ElastiCache para melhorar a latência e a taxa de transferência para cargas de trabalho de aplicativos com alto consumo de leitura**

**R: Use o Amazon ElastiCache para melhorar o desempenho de cargas de trabalho com uso intensivo de computação**

**Opção correta:**

- **Use o Amazon ElastiCache para melhorar a latência e a taxa de transferência para cargas de trabalho de aplicativos com alto consumo de leitura**
- **Use o Amazon ElastiCache para melhorar o desempenho de cargas de trabalho com uso intensivo de computação**

O Amazon ElastiCache permite que você execute armazenamentos de dados na memória na nuvem AWS. O Amazon ElastiCache é uma escolha popular para casos de uso em tempo real, como cache, armazenamentos de sessão, jogos, serviços geoespaciais, análises em tempo real e enfileiramento.

O Amazon ElastiCache pode ser usado para melhorar significativamente a latência e a taxa de transferência de muitas cargas de trabalho de aplicativos com uso intenso de leitura (como redes sociais, jogos, compartilhamento de mídia, tabelas de classificação e portais de perguntas e respostas) ou cargas de trabalho com uso intensivo de computação (como um mecanismo de recomendação), permitindo que você armazene os objetos que são lidos com frequência no cache.

#### **Pergunta 40**

Um líder de engenharia está projetando uma VPC com sub-redes públicas e privadas. A VPC e as sub-redes usam blocos CIDR IPv4. Há uma sub-rede pública e uma sub-rede privada em cada uma das três Zonas de Disponibilidade (AZs) para alta disponibilidade. Um gateway de internet é usado para fornecer acesso à internet para as sub-redes públicas. As sub-redes privadas precisam de acesso à internet para permitir que as instâncias do Amazon EC2 baixem atualizações de software.

**Qual das seguintes opções representa a solução correta para configurar o acesso à Internet para sub-redes privadas?**

**R: Configure três gateways NAT, um em cada sub-rede pública em cada AZ. Crie uma tabela de rotas personalizada para cada AZ que encaminhe tráfego não local para o gateway NAT em sua AZ.**

**Opção correta:**

- **Configure três gateways NAT, um em cada sub-rede pública em cada AZ. Crie uma tabela de rotas personalizada para cada AZ que encaminhe tráfego não local para o gateway NAT em sua AZ.**

Você pode usar um gateway de tradução de endereços de rede (NAT) para permitir que instâncias em uma sub-rede privada se conectem à Internet ou a outros serviços da AWS, mas impedir que a Internet inicie uma conexão com essas instâncias.

Para criar um gateway NAT, você precisa especificar a sub-rede pública na qual o gateway NAT deve residir. Você também precisa especificar um endereço IP elástico para associar ao gateway NAT ao criá-lo. O endereço IP elástico não pode ser alterado após a associação ao gateway NAT. Após criar um gateway NAT, você precisa atualizar a tabela de rotas associada a uma ou mais de suas sub-redes privadas para direcionar o tráfego da Internet para o gateway NAT. Isso permite que instâncias em suas sub-redes privadas se comuniquem com a Internet.

Cada gateway NAT é criado em uma Zona de Disponibilidade específica e implementado com redundância nessa zona.

Se você tiver recursos em várias Zonas de Disponibilidade e elas compartilharem um gateway NAT, e se a Zona de Disponibilidade do gateway NAT estiver inativa, os recursos nas outras Zonas de Disponibilidade perderão o acesso à internet. Para criar uma arquitetura independente de Zona de Disponibilidade, crie um gateway NAT em cada Zona de Disponibilidade e configure seu roteamento para garantir que os recursos usem o gateway NAT na mesma Zona de Disponibilidade.

#### Pergunta 41

A equipe de DevOps de uma empresa multinacional está ajudando suas subsidiárias a padronizar instâncias do Amazon EC2 usando a mesma Imagem de Máquina da Amazon (AMI). Algumas dessas subsidiárias estão na mesma região da AWS, mas usam contas diferentes, enquanto outras estão em regiões diferentes da AWS, mas usam a mesma conta da empresa controladora. A equipe de DevOps contratou você como arquiteto de soluções para este projeto.

Qual das seguintes opções você identificaria como CORRETA em relação aos recursos de uma Imagem de Máquina da Amazon (AMI)? (Selecione três)

**R: Você pode copiar uma Amazon Machine Image (AMI) entre regiões da AWS**

**R: Copiar uma imagem de máquina da Amazon (AMI) apoiada por um snapshot criptografado não pode resultar em um snapshot de destino não criptografado**

**R: Você pode compartilhar uma Amazon Machine Image (AMI) com outra conta AWS**

**Opções corretas:**

- **Você pode copiar uma Amazon Machine Image (AMI) entre regiões da AWS**
- **Você pode compartilhar uma Amazon Machine Image (AMI) com outra conta AWS**
- **Copiar uma imagem de máquina da Amazon (AMI) apoiada por um snapshot criptografado não pode resultar em um snapshot de destino não criptografado**

Uma Imagem de Máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. Uma AMI inclui o seguinte:

Um ou mais snapshots do Amazon EBS ou, para AMIs com suporte de armazenamento de instância, um modelo para o volume raiz da instância.

Permissões de inicialização que controlam quais contas da AWS podem usar a AMI para iniciar instâncias.

Um mapeamento de dispositivo de bloco que especifica os volumes a serem anexados à instância quando ela é iniciada.

Você pode copiar uma AMI dentro ou entre regiões da AWS usando o Console de Gerenciamento da AWS, a Interface de Linha de Comando da AWS ou SDKs, ou a API do Amazon EC2, todos compatíveis com a ação CopyImage. Você pode copiar AMIs baseadas no Amazon EBS e AMIs baseadas em armazenamento de instâncias. Você pode copiar AMIs com snapshots criptografados e também alterar o status da criptografia durante o processo de cópia. Portanto, a opção "Você pode copiar uma AMI entre regiões da AWS" está correta.

A tabela a seguir mostra o suporte à criptografia para vários cenários de cópia de AMI. Embora seja possível copiar um snapshot não criptografado para gerar um snapshot criptografado, não é possível copiar um snapshot criptografado para gerar um não criptografado. Portanto, a opção "Copiar uma AMI com suporte de um snapshot criptografado não pode resultar em um snapshot de destino não criptografado" está correta.

#### Pergunta 42

Uma empresa sofreu recentemente uma indisponibilidade de banco de dados em seu data center local. A empresa agora deseja migrar para uma solução de banco de dados confiável na AWS que minimize a perda de dados e armazene cada transação em pelo menos dois nós.

Qual das seguintes soluções atende a esses requisitos?

**R: Configurar uma instância do Amazon RDS MySQL DB com a funcionalidade Multi-AZ habilitada para replicar os dados de forma síncrona**

**Opção correta:**

- **Configurar uma instância do Amazon RDS MySQL DB com a funcionalidade Multi-AZ habilitada para replicar os dados de forma síncrona**



Ao provisionar uma Instância de Banco de Dados Multi-AZ do RDS, o Amazon RDS cria automaticamente uma Instância de Banco de Dados primária e replica os dados de forma síncrona para uma instância em espera em uma Zona de Disponibilidade (AZ) diferente. Cada AZ é executada em sua própria infraestrutura fisicamente distinta e independente, e foi projetada para ser altamente confiável. Executar uma instância de Banco de Dados com alta disponibilidade pode aumentar a disponibilidade durante a manutenção planejada do sistema e ajudar a proteger seus bancos de dados contra falhas na instância de Banco de Dados e interrupções na Zona de Disponibilidade. Em caso de indisponibilidade planejada ou não planejada da sua instância de Banco de Dados, o Amazon RDS alterna automaticamente para uma réplica em espera em outra Zona de Disponibilidade, se você tiver habilitado a Multi-AZ. O tempo necessário para a conclusão do failover depende da atividade do banco de dados e de outras condições no momento em que a instância de Banco de Dados primária ficou indisponível. Os tempos de failover normalmente variam de 60 a 120 segundos.

#### **Pergunta 43**

Uma empresa possui uma estrutura de nuvem híbrida para seu data center local e infraestrutura de Nuvem AWS. A empresa deseja construir uma solução de arquivamento de logs da web de forma que apenas os logs acessados com mais frequência estejam disponíveis como dados em cache localmente, enquanto todos os logs são armazenados em backup no Amazon S3.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria para este caso de uso?

**R: Use o AWS Volume Gateway - Volume em cache - para armazenar os logs acessados com mais frequência localmente para acesso de baixa latência enquanto armazena o volume completo com todos os logs em seu bucket de serviço Amazon S3**

**Opção correta:**

- **Use o AWS Volume Gateway - Volume em cache - para armazenar os logs acessados com mais frequência localmente para acesso de baixa latência enquanto armazena o volume completo com todos os logs em seu bucket de serviço Amazon S3**

O AWS Storage Gateway é um serviço de armazenamento em nuvem híbrida que oferece acesso local a armazenamento em nuvem praticamente ilimitado. O serviço oferece três tipos diferentes de gateways - Tape Gateway, File Gateway e Volume Gateway - que conectam perfeitamente aplicativos locais ao armazenamento em nuvem, armazenando dados em cache localmente para acesso de baixa latência. Com volumes em cache, o AWS Volume Gateway armazena o volume completo em seu bucket de serviço do Amazon S3, e apenas os dados acessados recentemente são retidos no cache local do gateway para acesso de baixa latência.

#### **Pergunta 44**

Uma empresa possui servidores de aplicativos na sub-rede pública que se conectam às instâncias do Amazon RDS na sub-rede privada. Para manutenção regular, as instâncias do Amazon RDS precisam de correções de patches que precisam ser baixadas da internet.

Considerando que a empresa usa apenas endereçamento IPv4 e está procurando um serviço totalmente gerenciado, qual das seguintes opções você sugeriria como solução ideal?

**R: Configurar um gateway de tradução de endereços de rede (gateway NAT) na sub-rede pública da VPC**

**Opção correta:**

- **Configurar um gateway de tradução de endereços de rede (gateway NAT) na sub-rede pública da VPC**

Você pode usar um gateway de Tradução de Endereços de Rede (gateway NAT) para permitir que instâncias em uma sub-rede privada se conectem à internet ou a outros serviços da AWS, mas impedir que a internet inicie uma conexão com essas instâncias. Para criar um gateway NAT, você deve especificar a sub-rede pública na qual o gateway NAT deve residir.

Você também deve especificar um endereço IP elástico para associar ao gateway NAT ao criá-lo. O endereço IP elástico não pode ser alterado após a associação ao gateway NAT. Após criar um gateway NAT, você deve atualizar a tabela de rotas associada a uma ou mais de suas sub-redes privadas para direcionar o tráfego da Internet para o gateway NAT. Isso permite que instâncias em suas sub-redes privadas se comuniquem com a Internet. Se você não precisar mais de um gateway NAT, poderá excluí-lo. Excluir um gateway NAT desassocia seu endereço IP elástico, mas não o libera da sua conta.

#### **Pergunta 45**

Uma empresa de serviços financeiros está migrando suas filas de mensagens de sistemas de middleware autogerenciados orientados a mensagens para o Amazon Simple Queue Service (Amazon SQS). A equipe de desenvolvimento da empresa deseja minimizar os custos de uso do Amazon SQS.

Como arquiteto de soluções, qual das seguintes opções você recomendaria para o caso de uso em questão?

**R: Use a pesquisa longa do SQS para recuperar mensagens de suas filas do Amazon SQS**

**Opção correta:**

- **Use a pesquisa longa do SQS para recuperar mensagens de suas filas do Amazon SQS**

O Amazon Simple Queue Service (Amazon SQS) é um serviço de enfileiramento de mensagens totalmente gerenciado que permite desacoplar e dimensionar microsserviços, sistemas distribuídos e aplicativos sem servidor.

O Amazon SQS oferece sondagens curtas e longas para receber mensagens de uma fila. Por padrão, as filas usam sondagens curtas. Com a sondagem curta, o Amazon SQS envia a resposta imediatamente, mesmo que a consulta não tenha encontrado mensagens. Com a sondagem longa, o Amazon SQS envia uma resposta após coletar pelo menos uma mensagem disponível, até o número máximo de mensagens especificado na solicitação. O Amazon SQS envia uma resposta vazia somente se o tempo de espera da sondagem expirar.

A pesquisa longa torna mais barato recuperar mensagens da fila do Amazon SQS assim que elas estiverem disponíveis. Usar a pesquisa longa pode reduzir o custo do SQS, pois você pode reduzir o número de recebimentos vazios.

#### **Pergunta 46**

A equipe de engenharia de uma empresa de mídia social deseja usar os alarmes do Amazon CloudWatch para recuperar automaticamente instâncias do Amazon EC2 caso sejam danificadas. A equipe contratou você como arquiteto de soluções para fornecer experiência no assunto.

Como arquiteto de soluções, qual das seguintes afirmações você identificaria como CORRETA em relação a esse processo de recuperação automática? (Selecione duas)

**R: Se sua instância tiver um endereço IPv4 público, ela o manterá após a recuperação**

**R: Uma instância recuperada é idêntica à instância original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados da instância**

**Opções corretas:**

Você pode criar um alarme do Amazon CloudWatch para recuperar automaticamente a instância do Amazon EC2 caso ela seja danificada devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para reparo. Instâncias encerradas não podem ser recuperadas. Uma instância recuperada é idêntica à instância original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados da instância. Se a instância danificada estiver em um grupo de posicionamento, a instância recuperada será executada nesse grupo. Se a sua instância tiver um endereço IPv4 público, ela o manterá após a recuperação. Durante a recuperação da instância, ela é migrada durante uma reinicialização da instância e todos os dados na memória são perdidos.

#### Pergunta 47

Uma empresa de comércio eletrônico implantou seu aplicativo em várias instâncias do Amazon EC2 configuradas em uma sub-rede privada usando IPv4. Essas instâncias do Amazon EC2 leem e gravam um enorme volume de dados de e para o Amazon S3 na mesma região da AWS. A empresa configurou o roteamento de sub-rede para direcionar todo o tráfego da internet por meio de um gateway de Tradução de Endereços de Rede (gateway NAT). A empresa deseja criar a solução com o melhor custo-benefício sem afetar a capacidade do aplicativo de se comunicar com o Amazon S3 ou a internet.

Como AWS Certified Solutions Architect Associate, qual das seguintes opções você recomendaria?

**R: Configurar um endpoint de gateway da VPC para o Amazon S3. Anexar uma política de endpoint ao endpoint. Atualizar a tabela de rotas para direcionar o tráfego com destino ao S3 para o endpoint da VPC.**

**Opção correta:**

- **Configurar um endpoint de gateway da VPC para o Amazon S3. Anexar uma política de endpoint ao endpoint. Atualizar a tabela de rotas para direcionar o tráfego com destino ao S3 para o endpoint da VPC.**

Os endpoints de gateway fornecem conectividade confiável ao Amazon S3 sem a necessidade de um gateway de internet ou um dispositivo NAT para sua VPC. Após criar o endpoint de gateway, você pode adicioná-lo como destino na sua tabela de rotas para o tráfego destinado da sua VPC ao Amazon S3. Não há custo adicional pelo uso de endpoints de gateway.

A política de endpoint da VPC para o endpoint do gateway controla o acesso ao Amazon S3 da VPC por meio do endpoint. A política padrão permite acesso total.

#### Pergunta 48

Uma empresa global de manufatura com instalações nos EUA, Europa e Ásia está projetando uma nova aplicação distribuída para otimizar seu fluxo de trabalho de compras. Os pedidos registrados em uma região da AWS devem ser visíveis para todas as regiões da AWS em um segundo ou menos. O banco de dados deve ser capaz de facilitar o failover com um Objetivo de Tempo de Recuperação (RTO) curto. O tempo de atividade da aplicação é fundamental para garantir que os processos de fabricação não sejam afetados.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução MAIS econômica?

**R: Provisionar o Banco de Dados Global do Amazon Aurora**

**Opção correta:**

- **Provisionar o Banco de Dados Global do Amazon Aurora**

Um banco de dados global Aurora oferece recursos de failover mais abrangentes do que o failover fornecido por um cluster de banco de dados Aurora padrão. Ao usar um banco de dados global Aurora, você pode se planejar e se recuperar de desastres com bastante rapidez. A recuperação de desastres normalmente é medida usando valores de RTO e RPO. Objetivo de tempo de recuperação (RTO) – O tempo que um sistema leva para retornar ao

estado operacional após um desastre. Em outras palavras, o RTO mede o tempo de inatividade. Para um banco de dados global Aurora, o RTO pode ser da ordem de minutos.

Objetivo de ponto de recuperação (RPO) – A quantidade de dados que pode ser perdida (medida em tempo). Para um banco de dados global Aurora, o RPO normalmente é medido em segundos.

Com um banco de dados global Aurora, você pode escolher entre duas abordagens diferentes para failover:

1. Failover planejado gerenciado – Este recurso destina-se a ambientes controlados, como cenários de teste de recuperação de desastres (DR), manutenção operacional e outros procedimentos operacionais planejados. O failover planejado gerenciado permite realocar o cluster de banco de dados primário do seu banco de dados global Aurora para uma das regiões secundárias. Como esse recurso sincroniza os clusters de banco de dados secundários com o primário antes de fazer qualquer outra alteração, o RPO é 0 (sem perda de dados).
2. Failover não planejado ("desanexar e promover") – Para se recuperar de uma interrupção não planejada, você pode executar um failover entre regiões para um dos secundários do seu banco de dados global Aurora. O RTO para esse processo manual depende da rapidez com que você consegue executar as tarefas listadas em Recuperando um banco de dados global do Amazon Aurora de uma interrupção não planejada. O RPO normalmente é medido em segundos, mas depende do atraso de replicação do armazenamento do Aurora na rede no momento da falha.

#### **Pergunta 49**

Uma empresa de TI utiliza filas do Amazon Simple Queue Service (Amazon SQS) para desacoplar os diversos componentes da arquitetura do aplicativo. Como os componentes de consumo precisam de mais tempo para processar mensagens do Amazon Simple Queue Service (Amazon SQS), a empresa deseja adiar a entrega de novas mensagens à fila por alguns segundos.

Como arquiteto de soluções, qual das seguintes soluções você sugeriria à empresa?

**R: Use filas de atraso para adiar a entrega de novas mensagens na fila por alguns segundos**

**Opção correta:**

- **Use filas de atraso para adiar a entrega de novas mensagens na fila por alguns segundos**

O Amazon Simple Queue Service (SQS) é um serviço de enfileiramento de mensagens totalmente gerenciado que permite desacoplar e dimensionar microsserviços, sistemas distribuídos e aplicativos sem servidor. O Amazon SQS oferece dois tipos de filas de mensagens. As filas padrão oferecem taxa de transferência máxima, ordenação de melhor esforço e entrega pelo menos uma vez. As filas FIFO do Amazon SQS são projetadas para garantir que as mensagens sejam processadas exatamente uma vez, na ordem exata em que são enviadas.

As filas de atraso permitem que você adie a entrega de novas mensagens para uma fila por vários segundos, por exemplo, quando seu aplicativo de consumidor precisa de tempo adicional para processar mensagens. Se você criar uma fila de atraso, todas as mensagens que você enviar para a fila permanecerão invisíveis para os consumidores durante o período de atraso. O atraso padrão (mínimo) para uma fila é 0 segundos. O máximo é 15 minutos.

#### **Pergunta 50**

Uma pequena empresa vinha executando seus sistemas de TI na infraestrutura local, mas agora planeja migrar para a Nuvem AWS para obter eficiência operacional.

Como arquiteto de soluções, você pode sugerir uma solução sem servidor econômica para seu aplicativo principal que tenha conteúdo estático e dinâmico?

**R: Hospede o conteúdo estático no Amazon S3 e use o AWS Lambda com o Amazon DynamoDB para a aplicação web sem servidor que processa conteúdo dinâmico. O Amazon CloudFront atuará como front-end do AWS Lambda para distribuição em diversas regiões.**

**Opção correta:**

- **Hospede o conteúdo estático no Amazon S3 e use o AWS Lambda com o Amazon DynamoDB para a aplicação web sem servidor que processa conteúdo dinâmico. O Amazon CloudFront atuará como front-end do AWS Lambda para distribuição em diversas regiões.**

O AWS Lambda com Amazon DynamoDB é a solução ideal para uma solução sem servidor. O Amazon CloudFront ajudará a aprimorar a experiência do usuário, fornecendo conteúdo em diferentes localizações geográficas com baixa latência. O Amazon S3 é uma maneira econômica e rápida de distribuir conteúdo estático para aplicações web.

#### **Pergunta 51**

Uma empresa de comércio eletrônico executa sua aplicação web em instâncias do Amazon EC2 em um grupo de Auto Scaling e está configurada para processar pedidos de consumidores em uma fila do Amazon Simple Queue Service (Amazon SQS) para processamento posterior. A equipe de DevOps observou que o desempenho da aplicação cai em caso de um pico repentino de pedidos recebidos.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria para abordar esse caso de uso?

**R: Use uma política de dimensionamento de rastreamento de destino com base em uma métrica de fila personalizada do Amazon SQS**

**Opção correta:**

- **Use uma política de dimensionamento de rastreamento de destino com base em uma métrica de fila personalizada do Amazon SQS**

Se você usar uma política de dimensionamento de rastreamento de destino baseada em uma métrica de fila personalizada do Amazon SQS, o dimensionamento dinâmico poderá se ajustar à curva de demanda do seu aplicativo com mais eficiência. Você pode usar uma métrica existente do Amazon SQS do CloudWatch, como `ApproximateNumberOfMessagesVisible`, para o rastreamento de destino, mas ainda poderá enfrentar um problema, fazendo com que o número de mensagens na fila não mude proporcionalmente ao tamanho do grupo de Auto Scaling que processa as mensagens da fila. A solução é usar uma métrica de backlog por instância, com o valor de destino sendo o backlog por instância aceitável a ser mantido.

Para calcular seu backlog por instância, divida o atributo de fila `ApproximateNumberOfMessages` pelo número de instâncias no estado `InService` para o grupo de Dimensionamento Automático. Em seguida, defina um valor-alvo para o backlog aceitável por instância.

Para ilustrar com um exemplo, digamos que o `ApproximateNumberOfMessages` atual seja 1500 e a capacidade de execução da frota seja 10. Se o tempo médio de processamento for de 0,1 segundo para cada mensagem e a latência máxima aceitável for de 10 segundos, o backlog aceitável por instância será  $10 / 0,1$ , que é igual a 100. Isso significa que 100 é o valor-alvo para sua política de rastreamento de metas. Se o backlog por instância estiver atualmente em 150 ( $1500 / 10$ ), sua frota será dimensionada horizontalmente, e será dimensionada em cinco instâncias para manter a proporção em relação ao valor-alvo.

#### **Pergunta 52**

Um aplicativo de videoconferência é hospedado em uma frota de instâncias do EC2 que fazem parte de um grupo de Auto Scaling. O grupo de Auto Scaling usa um Modelo de Lançamento (LT1) com localização de instância "dedicada", mas a VPC (V1) usada pelo Modelo de Lançamento LT1 tem a localização de instância definida como padrão. Posteriormente, a equipe de DevOps cria um novo Modelo de Lançamento (LT2) com localização de instância compartilhada (padrão), mas a VPC (V2) usada pelo Modelo de Lançamento LT2 tem a localização de instância definida como dedicada.

Qual das seguintes opções está correta em relação às instâncias iniciadas via Launch Template LT1 e Launch Template LT2?

**R: As instâncias lançadas pelo Launch Template LT1 e Launch Template LT2 terão locação de instância dedicada**

**Opção correta:**

- **As instâncias lançadas pelo Launch Template LT1 e Launch Template LT2 terão locação de instância dedicada**

Um modelo de inicialização especifica informações de configuração da instância. Ele inclui o ID da Imagem de Máquina da Amazon (AMI), o tipo de instância, um par de chaves, grupos de segurança e outros parâmetros usados para iniciar instâncias do EC2. Se você já iniciou uma instância do EC2 antes, especificou as mesmas informações para iniciá-la.

Ao criar um Modelo de Inicialização, o valor padrão para a locação da instância é compartilhado, e a locação da instância é controlada pelo atributo de locação da VPC. Se você definir a Locação do Modelo de Inicialização como compartilhada (padrão) e a Locação da VPC estiver definida como dedicada, as instâncias terão locação dedicada. Se você definir a Locação do Modelo de Inicialização como dedicada e a Locação da VPC estiver definida como padrão, as instâncias terão locação dedicada novamente.

O Amazon EC2 oferece três opções para a locação de suas instâncias do EC2:

**Compartilhado (Shared)** – Várias contas da AWS podem compartilhar o mesmo hardware físico. Esta é a opção de locação padrão ao iniciar uma instância.

**Instâncias dedicadas (Dedicated)** – Sua instância é executada em hardware de locatário único. Nenhum outro cliente da AWS compartilha o mesmo servidor físico.

**Hosts Dedicados (Host Dedicado)** – A instância é executada em um servidor físico dedicado ao seu uso. O uso de Hosts Dedicados facilita a aquisição de suas próprias licenças (BYOL) com requisitos de hardware dedicados para o EC2 e a conformidade com os casos de uso. Se você escolher esta opção, deverá fornecer um grupo de recursos de host para o grupo de recursos de host da Tenancy.

### **Pergunta 53**

Uma empresa de varejo utiliza a Nuvem AWS para gerenciar sua infraestrutura de TI. A empresa configurou o AWS Organizations para gerenciar diversos departamentos que administram suas contas AWS e utilizam recursos como instâncias do Amazon EC2 e bancos de dados do Amazon RDS. A empresa deseja fornecer VPCs compartilhadas e gerenciadas centralmente para todos os departamentos que utilizam aplicativos que exigem um alto grau de interconectividade.

**Como arquiteto de soluções, qual das seguintes opções você escolheria para facilitar este caso de uso?**

**R: Use o compartilhamento de VPC para compartilhar uma ou mais sub-redes com outras contas da AWS pertencentes à mesma organização pai das Organizações da AWS**

**Opção correta:**

- **Use o compartilhamento de VPC para compartilhar uma ou mais sub-redes com outras contas da AWS pertencentes à mesma organização pai das Organizações da AWS**

O compartilhamento de VPC (parte do Resource Access Manager) permite que várias contas da AWS criem seus recursos de aplicação, como instâncias do Amazon EC2, bancos de dados do Amazon RDS, clusters do Amazon Redshift e funções do AWS Lambda, em Nuvens Privadas Virtuais (VPCs) da Amazon compartilhadas e gerenciadas centralmente. Para configurar isso, a conta proprietária da VPC (proprietária) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização do AWS Organizations. Após o compartilhamento de uma sub-rede, os participantes podem visualizar, criar, modificar e excluir seus recursos de aplicação nas sub-redes compartilhadas com eles. Os participantes não podem visualizar, modificar ou excluir recursos que pertencem a outros participantes ou ao proprietário da VPC.

Você pode compartilhar Amazon VPCs para aproveitar o roteamento implícito dentro de uma VPC para aplicativos que exigem um alto grau de interconectividade e estão dentro dos mesmos limites de confiança. Isso reduz o número de VPCs que você cria e gerencia, enquanto usa contas separadas para faturamento e controle de acesso.

#### Pergunta 54

A equipe de engenharia de uma empresa deseja usar o Amazon Simple Queue Service (Amazon SQS) para desacoplar componentes da arquitetura do aplicativo subjacente. No entanto, a equipe está preocupada com o fato de os componentes vinculados à VPC acessarem o Amazon Simple Queue Service (Amazon SQS) pela internet pública.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria para abordar esse caso de uso?

**R: Use o endpoint da VPC para acessar o Amazon SQS**

**Opção correta:**

- **Use o endpoint da VPC para acessar o Amazon SQS**

Os clientes da AWS podem acessar o Amazon Simple Queue Service (Amazon SQS) a partir de sua Amazon Virtual Private Cloud (Amazon VPC) usando endpoints da VPC, sem usar IPs públicos e sem precisar navegar pela internet pública. Os endpoints da VPC para o Amazon SQS são alimentados pelo AWS PrivateLink, uma tecnologia escalável e altamente disponível que permite conectar sua VPC de forma privada aos serviços da AWS suportados.

Os endpoints da Amazon VPC são fáceis de configurar. Eles também fornecem conectividade confiável com o Amazon SQS sem a necessidade de um gateway de internet, uma instância de Network Address Translation (NAT), uma conexão VPN ou uma conexão com o AWS Direct Connect. Com os endpoints da VPC, os dados entre a fila da Amazon VPC e do Amazon SQS são transferidos dentro da rede da Amazon, ajudando a proteger suas instâncias do tráfego da internet.

O AWS PrivateLink simplifica a segurança dos dados compartilhados com aplicativos baseados em nuvem, eliminando a exposição dos dados à internet pública. O AWS PrivateLink fornece conectividade privada entre VPCs, serviços da AWS e aplicativos locais, com segurança na rede da Amazon. O AWS PrivateLink facilita a conexão de serviços entre diferentes contas e VPCs, simplificando significativamente a arquitetura de rede.

#### Pergunta 55

Um consultor de TI está ajudando uma pequena empresa a reformular sua infraestrutura tecnológica na Nuvem AWS. A empresa possui duas contas AWS e todos os recursos são provisionados na us-west-2 região. O consultor de TI está tentando iniciar uma instância do Amazon EC2 em cada uma das duas contas AWS, de forma que as instâncias estejam na mesma Zona de Disponibilidade (AZ) da us-west-2 região. Mesmo após selecionar a mesma sub-rede padrão (us-west-2a) ao iniciar as instâncias em cada uma das contas AWS, o consultor de TI percebe que as Zonas de Disponibilidade (AZs) ainda são diferentes.

Como arquiteto de soluções, qual das seguintes opções você sugeriria para resolver esse problema?

**R: Use o ID da Zona de Disponibilidade (AZ) para identificar exclusivamente as Zonas de Disponibilidade nas duas Contas da AWS**

**Opção correta:**

- **Use o ID da Zona de Disponibilidade (AZ) para identificar exclusivamente as Zonas de Disponibilidade nas duas Contas da AWS**

Uma Zona de Disponibilidade é representada por um código de região seguido por um identificador alfabético; por exemplo, us-east-1a. Para garantir que os recursos sejam distribuídos entre as Zonas de Disponibilidade de uma região, a AWS mapeia as Zonas de Disponibilidade para os nomes de cada conta da AWS. Por exemplo, a Zona de Disponibilidade us-west-2a de uma conta da AWS pode não estar no mesmo local que us-west-2aa de outra conta da AWS.

Para coordenar Zonas de Disponibilidade entre contas, você deve usar o ID da AZ, que é um identificador único e consistente para uma Zona de Disponibilidade. Por exemplo, usw2-az2 é um ID da AZ para a us-west-2 região e tem a mesma localização em todas as contas da

AWS.

Visualizar IDs de AZ permite determinar a localização dos recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na Zona de Disponibilidade com o ID de AZ usw2-az2com outra conta, essa sub-rede estará disponível para a conta na Zona de Disponibilidade cujo ID de AZ também seja usw2-az2.

Você pode visualizar os IDs de AZ acessando a seção de integridade do serviço do Painel do Amazon EC2 por meio do AWS Management Console.

#### Pergunta 56

Uma empresa de serviços financeiros deseja identificar quaisquer dados confidenciais armazenados em seus buckets do Amazon S3. A empresa também deseja monitorar e proteger todos os dados armazenados no Amazon S3 contra qualquer atividade maliciosa.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria para ajudar a atender aos requisitos fornecidos?

**R: Use o Amazon GuardDuty para monitorar qualquer atividade maliciosa em dados armazenados no Amazon S3. Use o Amazon Macie para identificar quaisquer dados confidenciais armazenados no Amazon S3.**

**Opção correta:**

- **Use o Amazon GuardDuty para monitorar qualquer atividade maliciosa em dados armazenados no Amazon S3. Use o Amazon Macie para identificar quaisquer dados confidenciais armazenados no Amazon S3.**

O Amazon GuardDuty oferece detecção de ameaças que permite monitorar e proteger continuamente suas contas da AWS, cargas de trabalho e dados armazenados no Amazon S3. O GuardDuty analisa fluxos contínuos de metadados gerados a partir da sua conta e da atividade de rede encontrados em Eventos do AWS CloudTrail, Logs de Fluxo da Amazon VPC e Logs de DNS. Ele também utiliza inteligência integrada contra ameaças, como endereços IP maliciosos conhecidos, detecção de anomalias e aprendizado de máquina para identificar ameaças com mais precisão.

O Amazon Macie é um serviço de privacidade e segurança de dados totalmente gerenciado que usa aprendizado de máquina e correspondência de padrões para descobrir e proteger seus dados confidenciais no Amazon S3. O Macie detecta automaticamente uma lista grande e crescente de tipos de dados confidenciais, incluindo informações de identificação pessoal (PII), como nomes, endereços e números de cartão de crédito. Ele também oferece visibilidade constante da segurança e privacidade de dados dos seus dados armazenados no Amazon S3.

#### Pergunta 57

Seu aplicativo está hospedado por um provedor em yourapp.provider.com. Você gostaria que seus usuários acessassem seu aplicativo usando www.your-domain.com, que você possui e gerencia no Amazon Route 53.

Qual registro do Amazon Route 53 você deve criar?

**R: Criar um registro CNAME**

**Opção correta:**

- **Criar um registro CNAME**

Um registro CNAME mapeia consultas DNS para o nome do registro atual, como acme.example.com, para outro domínio (example.com ou example.net) ou subdomínio (acme.example.com ou zenith.example.org).

Registros CNAME podem ser usados para mapear um nome de domínio para outro. No entanto, lembre-se de que o protocolo DNS não permite a criação de um registro CNAME para o nó superior de um namespace DNS, também conhecido como apex de zona. Por exemplo, se você registrar o nome DNS example.com, o apex de zona será example.com. Você não pode criar um registro CNAME para example.com, mas pode criar registros CNAME para www.example.com,



newproduct.example.com e assim por diante.

#### **Pergunta 58**

A equipe de DevOps de uma empresa de TI está provisionando uma aplicação de duas camadas em uma VPC com uma sub-rede pública e uma sub-rede privada. A equipe deseja usar uma instância de Tradução de Endereços de Rede (NAT) ou um gateway de Tradução de Endereços de Rede (NAT) na sub-rede pública para permitir que instâncias na sub-rede privada iniciem tráfego IPv4 de saída para a internet, mas precisa de assistência técnica em relação às opções de configuração disponíveis para a instância de Tradução de Endereços de Rede (NAT) e o gateway de Tradução de Endereços de Rede (NAT).

Como arquiteto de soluções, qual das seguintes opções você identificaria como CORRETA? (Selecione três)

**R: A instância NAT pode ser usada como um servidor bastião**

**R: Grupos de segurança podem ser associados a uma instância NAT** **R: A instância NAT suporta encaminhamento de porta**

**Opções corretas:**

- **A instância NAT pode ser usada como um servidor bastião**
- **Grupos de segurança podem ser associados a uma instância NAT**
- **A instância NAT suporta encaminhamento de porta**

Uma instância NAT ou um Gateway NAT pode ser usado em uma sub-rede pública na sua VPC para permitir que instâncias na sub-rede privada iniciem tráfego IPv4 de saída para a Internet.

Veja este resumo de alto nível das diferenças entre instâncias NAT e gateways NAT relevantes para as opções descritas na pergunta:

#### **Pergunta 59**

Uma empresa farmacêutica global deseja mover a maioria dos dados locais para o Amazon S3, Amazon Elastic File System (Amazon EFS) e Amazon FSx for Windows File Server de forma fácil, rápida e econômica.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria como a MELHOR opção para automatizar e acelerar transferências de dados online para esses serviços de armazenamento da AWS?

**R: Use o AWS DataSync para automatizar e acelerar as transferências de dados on-line para os serviços de armazenamento da AWS fornecidos**

**Opção correta:**

- **Use o AWS DataSync para automatizar e acelerar as transferências de dados on-line para os serviços de armazenamento da AWS fornecidos**

O AWS DataSync é um serviço de transferência de dados on-line que simplifica, automatiza e acelera a cópia de grandes quantidades de dados de e para serviços de armazenamento da AWS pela Internet ou pelo AWS Direct Connect.

O AWS DataSync automatiza e acelera totalmente a migração de grandes conjuntos de dados ativos para a AWS, até 10 vezes mais rápido do que ferramentas de linha de comando. Ele é integrado nativamente ao Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon CloudWatch e AWS CloudTrail, o que proporciona acesso seguro e contínuo aos seus serviços de armazenamento, além de monitoramento detalhado da transferência.

O AWS DataSync utiliza um protocolo de rede específico e uma arquitetura escalável para transferir dados. Um único agente DataSync é capaz de saturar um link de rede de 10 Gbps.

O AWS DataSync automatiza totalmente a transferência de dados. Ele inclui mecanismos de nova tentativa e resiliência de rede, otimizações de rede, agendamento de tarefas integrado, monitoramento via API e Console do DataSync, além de métricas, eventos e logs

do Amazon CloudWatch que fornecem visibilidade granular do processo de transferência. O AWS DataSync realiza a verificação da integridade dos dados durante e ao final da transferência.

#### Pergunta 60

Uma empresa de streaming de mídia está buscando migrar sua infraestrutura local para a Nuvem AWS. A equipe de engenharia busca um armazenamento de dados persistente NoSQL totalmente gerenciado com cache na memória para manter a baixa latência, essencial para cenários em tempo real, como streaming de vídeo e conteúdo interativo. A equipe espera que o número de usuários simultâneos chegue a um milhão, para que o banco de dados possa ser escalável de forma elástica.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você recomendaria para este caso de uso?

**R: Amazon DynamoDB**

**Opção correta:**

- **Amazon DynamoDB**

O Amazon DynamoDB é um banco de dados de chave-valor e documentos que oferece desempenho de milissegundos em qualquer escala. É um banco de dados totalmente gerenciado, multirregional, multimestre e durável, com segurança integrada, backup e restauração e cache na memória para aplicativos em escala de internet. O DAX é um serviço de cache compatível com o DynamoDB que permite que você se beneficie de um desempenho rápido na memória para aplicativos exigentes. As empresas usam o cache por meio do DynamoDB Accelerator (DAX) quando têm altos volumes de leitura ou precisam de latência de leitura abaixo de um milissegundo.

#### Pergunta 61

Uma startup de mídia social utiliza a Nuvem AWS para gerenciar sua infraestrutura de TI. A equipe de engenharia da startup deseja realizar rollovers semanais de banco de dados para um servidor MySQL usando uma tarefa cron sem servidor que normalmente leva cerca de 5 minutos para executar o script de rollover do banco de dados escrito em Python. O rollover do banco de dados arquivará os dados da semana anterior do banco de dados de produção para manter o banco de dados pequeno e, ao mesmo tempo, manter seus dados acessíveis. Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução MAIS econômica e confiável?

**R: Agende uma expressão cron de evento semanal do Amazon EventBridge para invocar uma função do AWS Lambda que executa o trabalho de rollover do banco de dados**

**Opção correta:**

- **Agende uma expressão cron de evento semanal do Amazon EventBridge para invocar uma função do AWS Lambda que executa o trabalho de rollover do banco de dados**

O AWS Lambda permite que você execute código sem provisionar ou gerenciar servidores. Você paga apenas pelo tempo de computação que consome. O AWS Lambda suporta expressões cron e taxa padrão para frequências de até uma vez por minuto.

#### Pergunta 62

O backend do banco de dados para o site de uma empresa de varejo está hospedado no Amazon RDS para MySQL, com uma instância primária e três réplicas de leitura para oferecer suporte à escalabilidade de leitura. A empresa determinou que as réplicas de leitura não devem ter mais de 1 segundo de atraso em relação à instância primária para proporcionar a melhor experiência possível ao usuário. As réplicas de leitura estão ficando ainda mais atrasadas durante os períodos de pico de tráfego, resultando em uma experiência ruim para o usuário, pois as pesquisas produzem resultados inconsistentes.

Você foi contratado como Arquiteto de Soluções Certificado pela AWS - Associado para reduzir o atraso de replicação o máximo possível com alterações mínimas no código do aplicativo ou no esforço necessário para gerenciar os recursos subjacentes.

Qual das opções a seguir você recomendaria?

**R: Configurar a migração do banco de dados do Amazon RDS MySQL para o Amazon Aurora MySQL. Trocar as réplicas de leitura do MySQL por réplicas do Aurora. Configurar o Auto**

## Scaling do Aurora.

### Opção correta:

- **Configurar a migração do banco de dados do Amazon RDS MySQL para o Amazon Aurora MySQL. Trocar as réplicas de leitura do MySQL por réplicas do Aurora. Configurar o Auto Scaling do Aurora.**

O Aurora apresenta um sistema de armazenamento distribuído, tolerante a falhas e autocorretivo, desacoplado dos recursos computacionais e com dimensionamento automático de até 128 TiB por instância de banco de dados. Ele oferece alto desempenho e disponibilidade com até 15 réplicas de leitura de baixa latência, recuperação pontual, backup contínuo no Amazon Simple Storage Service (Amazon S3) e replicação em três Zonas de Disponibilidade (AZs).

Como as réplicas do Amazon Aurora compartilham o mesmo volume de dados que a instância primária na mesma região da AWS, praticamente não há atraso de replicação. Os tempos de atraso da réplica são da ordem de dezenas de milissegundos (em comparação com o atraso de replicação de segundos no caso de réplicas de leitura do MySQL). Portanto, esta é a opção certa para garantir que as réplicas de leitura não fiquem mais de 1 segundo atrás da instância primária.

### Pergunta 63

Uma startup de mídia está procurando hospedar seu aplicativo da web na AWS Cloud. O aplicativo será acessado por usuários de diferentes regiões geográficas do mundo para carregar e baixar arquivos de vídeo que podem atingir um tamanho máximo de 10 gigabytes. A startup quer que a solução seja econômica e escalável com a menor latência possível para uma ótima experiência do usuário.

Como arquiteto de soluções, qual das opções a seguir você sugeriria como solução ideal para atender aos requisitos fornecidos?

**R: Use o Amazon S3 para hospedar o aplicativo da web e use o Amazon S3 Transfer Acceleration (Amazon S3TA) para reduzir a latência que usuários geograficamente dispersos podem enfrentar**

### Opção correta:

- **Use o Amazon S3 para hospedar o aplicativo da web e use o Amazon S3 Transfer Acceleration (Amazon S3TA) para reduzir a latência que usuários geograficamente dispersos podem enfrentar**

O Amazon S3 Transfer Acceleration (S3TA) pode acelerar as transferências de conteúdo de e para o Amazon S3 em até 50% a 500% para transferências de longa distância de objetos maiores. Clientes que possuem aplicativos web ou móveis com usuários espalhados ou aplicativos hospedados longe de seu bucket S3 podem experimentar velocidades de upload e download longas e variáveis pela internet. O S3 Transfer Acceleration (S3TA) reduz a variabilidade no roteamento, no congestionamento e nas velocidades da internet que podem afetar as transferências, e logicamente encurta a distância até o S3 para aplicativos remotos. O S3TA melhora o desempenho de transferência ao rotear o tráfego pelos Edge Locations distribuídos globalmente do Amazon CloudFront e pelas redes de backbone da AWS, além de usar otimizações de protocolo de rede.

Para aplicativos que interagem com seus buckets do Amazon S3 por meio da API do S3 de fora da região do seu bucket, o S3TA ajuda a evitar a variabilidade no roteamento e o congestionamento da internet. Ele faz isso roteando seus uploads e downloads pela infraestrutura de rede global da AWS, para que você se beneficie das otimizações de rede da AWS.

### Pergunta 64

Uma empresa de mídia quer uma maneira de baixa latência para distribuir resultados

esportivos ao vivo, que são entregues por meio de um aplicativo proprietário usando o protocolo UDP. Como arquiteto de soluções, qual das seguintes soluções você recomendaria para oferecer o MELHOR desempenho para este caso de uso?

**R: Use o AWS Global Accelerator para fornecer uma maneira de baixa latência para distribuir resultados esportivos ao vivo**

**Opção correta:**

- **Use o AWS Global Accelerator para fornecer uma maneira de baixa latência para distribuir resultados esportivos ao vivo**

O AWS Global Accelerator é um serviço de rede que ajuda a melhorar a disponibilidade e o desempenho dos aplicativos oferecidos aos seus usuários globais. O AWS Global Accelerator é fácil de instalar, configurar e gerenciar. Ele fornece endereços IP estáticos que proporcionam um ponto de entrada fixo para seus aplicativos e eliminam a complexidade de gerenciar endereços IP específicos para diferentes regiões e zonas de disponibilidade (AZs) da AWS. O AWS Global Accelerator sempre encaminha o tráfego do usuário para o endpoint ideal com base no desempenho, reagindo instantaneamente a alterações na integridade do aplicativo, na localização do usuário e nas políticas configuradas. O Global Accelerator é uma boa opção para casos de uso não HTTP, como jogos (UDP), IoT (MQTT) ou Voz sobre IP. Portanto, esta opção está correta.

#### **Alerta de exame:**

Observe as diferenças entre os recursos do AWS Global Accelerator e do Amazon CloudFront - O AWS Global Accelerator e o Amazon CloudFront são serviços separados que usam a rede global da AWS e seus locais de borda ao redor do mundo. O Amazon CloudFront melhora o desempenho para conteúdo armazenável em cache (como imagens e vídeos) e conteúdo dinâmico (como aceleração de API e entrega dinâmica de site). O AWS Global Accelerator melhora o desempenho para uma ampla gama de aplicativos sobre TCP ou UDP, fazendo proxy de pacotes na borda para aplicativos em execução em uma ou mais regiões da AWS.

O AWS Global Accelerator é uma boa opção para casos de uso não HTTP, como jogos (UDP), IoT (MQTT) ou Voz sobre IP, bem como para casos de uso HTTP que exigem especificamente endereços IP estáticos ou failover regional rápido e determinístico. Ambos os serviços se integram ao AWS Shield para proteção contra DDoS.

#### **Pergunta 65**

Uma empresa de TI hospeda aplicativos baseados em Windows em seu data center local. A empresa está considerando migrar os negócios para a Nuvem AWS. A solução em nuvem deve oferecer espaço de armazenamento compartilhado que múltiplos aplicativos possam acessar sem a necessidade de replicação. Além disso, a solução deve se integrar ao domínio autogerenciado do Active Directory da empresa.

Qual das seguintes soluções atende a esses requisitos com o mínimo esforço de integração?

**R: Use o Amazon FSx para Windows File Server como uma solução de armazenamento compartilhado**

**Opção correta:**

- **Use o Amazon FSx para Windows File Server como uma solução de armazenamento compartilhado**  
O Amazon FSx for Windows File Server oferece armazenamento de arquivos totalmente gerenciado, altamente confiável e escalável, acessível através do protocolo SMB (Server Message Block), padrão do setor. Ele é baseado no Windows Server e oferece uma ampla gama de recursos administrativos, como cotas de usuários, restauração de arquivos de usuários finais e integração com o Microsoft Active Directory (AD). Oferece opções de implantação em uma ou várias zonas de disponibilidade (AZ), backups totalmente gerenciados e criptografia de dados em repouso e em trânsito. Você pode otimizar custos e desempenho para suas necessidades de carga de trabalho com opções de armazenamento em SSD e HDD; e pode dimensionar o armazenamento e alterar o desempenho da taxa de transferência do seu sistema de arquivos a qualquer momento.

Com o Amazon FSx, você obtém armazenamento de arquivos altamente disponível e durável a partir de US\$ 0,013 por GB/mês. A deduplicação de dados permite otimizar ainda mais os custos, removendo dados redundantes. Você pode aumentar o armazenamento do seu sistema de

arquivos e dimensionar a capacidade de transferência a qualquer momento, facilitando a resposta às mudanças nas necessidades dos negócios. Não há custos iniciais nem taxas de licenciamento.