

Pergunta 1

Uma empresa de serviços financeiros tradicionalmente opera com um data center local e gostaria de criar uma estratégia de recuperação de desastres aproveitando a Nuvem AWS.

Como um Solutions Architect, você gostaria de garantir que uma versão reduzida de um ambiente totalmente funcional esteja sempre em execução na nuvem da AWS e, em caso de desastre, o tempo de recuperação seja mantido no mínimo. Qual estratégia de recuperação de desastre é essa?

R: Espera Quente

Opção correta:

Espera Quente

O termo "warm standby" é usado para descrever um cenário de recuperação de desastres (DR) no qual uma versão reduzida de um ambiente totalmente funcional está sempre em execução na nuvem. Uma solução de "warm standby" estende os elementos da luz piloto e a preparação. Ela reduz ainda mais o tempo de recuperação, pois alguns serviços estão sempre em execução. Ao identificar seus sistemas críticos para os negócios, você pode duplicá-los completamente na AWS e mantê-los sempre ativos.

Pergunta 2

Uma pequena empresa de locação tinha 5 funcionários, todos trabalhando na mesma conta de nuvem da AWS. Esses funcionários implantaram seus aplicativos desenvolvidos para diversas funções, incluindo faturamento, operações, finanças, etc. Cada um desses funcionários operava em sua própria VPC. Agora, é necessário conectar essas VPCs para que os aplicativos possam se comunicar entre si. Qual das seguintes opções é a solução MAIS econômica para este caso de uso?

R: Use uma conexão de peering VPC

Opção correta:

Use uma conexão de peering VPC

Uma conexão de peering de VPC é uma conexão de rede entre duas VPCs que permite rotear o tráfego entre elas usando endereços IPv4 privados ou IPv6. Instâncias em qualquer uma das VPCs podem se comunicar entre si como se estivessem na mesma rede. Você pode criar uma conexão de peering de VPC entre suas próprias VPCs ou com uma VPC em outra conta da AWS. As VPCs podem estar em regiões diferentes (também conhecido como conexão de peering de VPC inter-regional). O peering de VPC ajuda a conectar duas VPCs e não é transitivo. Para conectar VPCs, a melhor opção disponível é usar o peering de VPC.

Pergunta 3

Como arquiteto de soluções, você criou uma solução que utiliza um Application Load Balancer com stickiness e um Auto Scaling Group (ASG). O Auto Scaling Group abrange 2 Availability Zones (AZs). AZ-A tem 3 instâncias do Amazon EC2 e AZ-B tem 4 instâncias do Amazon EC2. O Auto Scaling Group está prestes a entrar em um evento de scale-in devido ao acionamento de um alarme do Amazon CloudWatch.

O que acontecerá na configuração padrão do Grupo de Dimensionamento Automático?

R: A instância com o modelo de inicialização ou configuração de inicialização mais antigo será encerrada em AZ-B

Opção correta:

A instância com o modelo de inicialização ou configuração de inicialização mais antigo será encerrada em AZ-B

O Amazon EC2 Auto Scaling ajuda a garantir que você tenha o número de instâncias do Amazon EC2 disponíveis para lidar com a carga do seu aplicativo. Você cria coleções de instâncias do Amazon EC2, chamadas de grupos de Auto Scaling. Você pode especificar o número mínimo de instâncias em

cada grupo de Auto Scaling, e o Amazon EC2 Auto Scaling garante que seu grupo nunca fique abaixo desse tamanho.

Com cada grupo de dimensionamento automático, você pode controlar quando ele adiciona instâncias (chamado de dimensionamento horizontal) ou remove instâncias (chamado de dimensionamento vertical) da sua arquitetura de rede.

A política de encerramento padrão foi criada para ajudar a garantir que suas instâncias abranjam Zonas de Disponibilidade uniformemente para alta disponibilidade. A política padrão é genérica e flexível para abranger uma variedade de cenários.

O comportamento da política de encerramento padrão é o seguinte: 1. Determine quais Zonas de Disponibilidade (Azs) têm mais instâncias e pelo menos uma instância que não está protegida contra redução. 2. Determine quais instâncias encerrar para alinhar as instâncias restantes à estratégia de alocação para a Instância On-Demand ou Spot que está sendo encerrada. 3. Determine se alguma das instâncias usa o modelo ou configuração de inicialização mais antigo: 3.a. Determine se alguma das instâncias usa o modelo de inicialização mais antigo, a menos que haja instâncias que usem uma configuração de inicialização. 3.b. Determine se alguma das instâncias usa a configuração de inicialização mais antiga. 4. Depois de aplicar todos os critérios acima, se houver várias

instâncias desprotegidas para encerrar, determine quais instâncias estão mais próximas da próxima hora de cobrança.

Conforme o caso de uso fornecido, as AZs serão balanceadas primeiro e, em seguida, a instância com o modelo de inicialização ou configuração de inicialização mais antigo dentro da AZ aplicável (**AZ-B**) será encerrada.

Pergunta 4

Uma empresa de comércio eletrônico rastreia os cliques dos usuários em seu site principal e realiza análises para fornecer recomendações de produtos quase em tempo real. Uma instância do Amazon EC2 recebe dados do site e os envia para uma instância do Amazon Aurora Database. Outra instância do Amazon EC2 verifica continuamente as alterações no banco de dados e executa consultas SQL para fornecer recomendações. Agora, a empresa deseja um redesenho para desacoplar e escalar a infraestrutura. A solução deve garantir que os dados possam ser analisados em tempo real sem perda de dados, mesmo quando a empresa observa grandes picos de tráfego.

O que você recomendaria como Arquiteto de Soluções Certificado pela AWS - Associado?

R: Utilize o Amazon Kinesis Data Streams para capturar os dados do site e inseri-los no Amazon Kinesis Data Analytics, que pode consultá-los em tempo real. Por fim, o feed analisado é enviado ao Amazon Kinesis Data Firehose para persistir os dados no Amazon S3.

Opção correta:

Utilize o Amazon Kinesis Data Streams para capturar os dados do site e inseri-los no Amazon Kinesis Data Analytics, que pode consultá-los em tempo real. Por fim, o feed analisado é enviado ao Amazon Kinesis Data Firehose para persistir os dados no Amazon S3.

Você pode usar o Amazon Kinesis Data Streams para criar aplicativos personalizados que processam ou analisam dados de streaming para necessidades específicas. O Amazon Kinesis Data Streams gerencia a infraestrutura, o armazenamento, a rede e a configuração necessários para transmitir seus dados no nível da sua taxa de transferência. Você não precisa se preocupar com provisionamento, implantação ou manutenção contínua de hardware, software ou outros serviços para seus fluxos de dados.

Para o caso de uso fornecido, você pode usar o Amazon Kinesis Data Analytics para transformar e analisar dados de streaming de entrada do Kinesis Data Streams em tempo real. O Kinesis Data Analytics cuida de tudo o que é necessário para executar aplicativos de streaming continuamente e dimensiona automaticamente para corresponder ao volume e à taxa de transferência dos seus dados de entrada. Com o Amazon Kinesis Data Analytics, não há servidores para gerenciar, nenhuma taxa mínima ou custo de configuração, e você paga apenas pelos recursos que seus aplicativos de streaming consomem.

O Amazon Kinesis Data Firehose é um serviço de extração, transformação e carregamento (ETL) que captura, transforma e entrega dados de streaming de forma confiável para data lakes, armazenamentos de dados e serviços de análise.

Para o caso de uso fornecido, após a análise em tempo real, o feed de saída do Kinesis Data Analytics é enviado para o Kinesis Data Firehose, que despeja os dados no Amazon S3 sem nenhuma perda de dados.

Pergunta 5

Uma empresa desenvolveu uma aplicação serverless usando o Amazon API Gateway e o AWS Lambda. O backend utiliza um banco de dados MySQL do Amazon Aurora. A aplicação web foi lançada inicialmente nas Américas e a empresa agora gostaria de expandi-la para a Europa, onde uma versão somente leitura estará disponível para melhorar a latência. Você planeja implantar o Amazon API Gateway e o AWS Lambda usando o AWS CloudFormation, mas gostaria de ter uma cópia somente leitura dos seus dados também na Europa.

Como arquiteto de soluções, o que você recomenda?

R: Use réplicas de leitura do Amazon Aurora

Opção correta:

Use réplicas de leitura do Amazon Aurora

O Amazon Aurora oferece um sistema de armazenamento distribuído, tolerante a falhas e autocorretivo, com dimensionamento automático para até 64 TB 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 S3 e replicação em três Zonas de Disponibilidade (AZs).

Réplicas do Aurora são endpoints independentes em um cluster de banco de dados do Aurora, mais indicados para escalar operações de leitura. Até 15 Réplicas do Aurora podem ser distribuídas entre as Zonas de Disponibilidade (AZs) que um cluster de banco de dados abrange em uma região da AWS. O volume do cluster de banco de dados é composto por várias cópias dos dados do cluster de banco de dados. No entanto, os dados no volume do cluster são representados como um único volume lógico para a instância primária e as Réplicas do Aurora no cluster de banco de dados. Você também pode configurar dois clusters de banco de dados do Aurora MySQL em diferentes regiões da AWS, criando uma Réplica de Leitura do Aurora de um cluster de banco de dados do Amazon Aurora MySQL em uma região diferente da AWS. Dessa forma, as Réplicas de Leitura do Aurora podem ser implantadas globalmente.

Pergunta 6

Você começou um novo emprego como arquiteto de soluções em uma empresa que tem especialistas em AWS e pessoas aprendendo AWS. Recentemente, um desenvolvedor configurou incorretamente um banco de dados Amazon RDS recém-criado, o que resultou em uma interrupção da produção.

Como você pode garantir que as práticas recomendadas específicas do Amazon RDS sejam incorporadas em um modelo de infraestrutura reutilizável para ser usado por todos os seus usuários da AWS?

R: Use o AWS CloudFormation para gerenciar bancos de dados do Amazon RDS

Opção correta:

Use o AWS CloudFormation para gerenciar bancos de dados do Amazon RDS

O AWS CloudFormation fornece uma linguagem comum para você modelar e provisionar recursos de aplicativos da AWS e de terceiros em seu ambiente de nuvem. O AWS CloudFormation permite que você use linguagens de programação ou um arquivo de texto simples para modelar e provisionar, de forma automatizada e segura, todos os recursos necessários para seus aplicativos em todas as regiões e contas. Isso lhe dá uma única fonte de verdade para seus recursos da AWS e de terceiros.

O AWS CloudFormation permite que você mantenha sua infraestrutura como código e reutilize as melhores práticas em sua empresa para parâmetros de configuração. Portanto, esta é a opção correta para o caso de uso fornecido.

Pergunta 7

Você trabalha como arquiteto da AWS para uma instalação de monitoramento meteorológico. Você precisa configurar um mecanismo de Recuperação de Desastres (DR) com custos mínimos. Em caso de falha, a instalação só pode suportar uma perda de dados de aproximadamente 15 minutos sem comprometer os modelos de previsão.

Como arquiteto de soluções, qual método de DR você sugeriria?

R: Luz piloto

Opção correta:

Luz piloto

O termo "piloto de luz" é frequentemente usado para descrever um cenário de recuperação de desastres (DR) no qual uma versão mínima de um ambiente está sempre em execução na nuvem. A ideia do piloto de luz é uma analogia que vem do aquecedor a gás. Em um aquecedor a gás, uma pequena chama sempre acesa pode rapidamente acender todo o aquecedor para aquecer uma casa. Este cenário é semelhante a um cenário de backup e restauração. Por exemplo, com a AWS, você pode manter um piloto de luz configurando e executando os elementos centrais mais críticos do seu sistema na AWS. Para o caso de uso em questão, uma pequena parte da infraestrutura de backup está sempre em execução

simultaneamente, sincronizando dados mutáveis (como bancos de dados ou documentos) para que não haja perda de dados críticos. Quando chegar a hora da recuperação, você poderá provisionar rapidamente um ambiente de produção em larga escala em torno do núcleo crítico. Para o piloto de luz, o RPO/RTO é em dezenas de minutos, então esta é a solução correta.

Pergunta 8

A lógica de negócios de uma empresa é baseada em vários microsserviços executados no data center local. Atualmente, eles se comunicam por meio de um agente de mensagens compatível com o protocolo MQTT. A empresa está considerando migrar esses aplicativos e o agente de mensagens para a Nuvem AWS sem alterar a lógica do aplicativo. Qual tecnologia permite que você obtenha um agente de mensagens gerenciado que suporta o protocolo MQTT?

R: Amazon MQ

Opção correta:

Amazon MQ

O Amazon MQ é um serviço gerenciado de r de mensagens para o Apache ActiveMQ que facilita a configuração e a operação de res de mensagens na nuvem. Os res de mensagens permitem que diferentes sistemas de software – geralmente usando diferentes linguagens de programação e em diferentes plataformas – se comuniquem e troquem informações. Se uma organização utiliza mensagens com aplicativos existentes e deseja migrar o serviço de mensagens para a nuvem de forma rápida e fácil, a AWS recomenda o Amazon MQ para esse caso de uso. Conectar seus aplicativos atuais ao Amazon MQ é fácil porque ele utiliza APIs e protocolos padrão do setor para mensagens, incluindo JMS, NMS, AMQP, STOMP, MQTT e WebSocket.

Portanto, a única resposta possível é o Amazon MQ.

Pergunta 9

A equipe de engenharia de uma empresa de mídia social migrou recentemente para a AWS Cloud de seu data center local. A equipe está avaliando o Amazon CloudFront para ser usado como um CDN para seu aplicativo principal. A equipe contratou você como um AWS Certified Solutions Architect – Associate para aconselhar sobre os recursos do Amazon CloudFront em roteamento, segurança e alta disponibilidade.

Qual das seguintes opções você identificaria como correta em relação ao Amazon CloudFront? (Selecione três)

R: O Amazon CloudFront pode rotear para várias origens com base no tipo de conteúdo

R: Use um grupo de origem com origens primárias e secundárias para configurar o Amazon CloudFront para alta disponibilidade e failover

R: Use criptografia em nível de campo no Amazon CloudFront para proteger dados confidenciais para conteúdo específico

Opções corretas:

O Amazon CloudFront pode rotear para várias origens com base no tipo de conteúdo

Você pode configurar uma única distribuição web do Amazon CloudFront para atender a diferentes tipos de solicitações de várias origens. Por exemplo, se você estiver criando um site que atende a conteúdo estático de um bucket do Amazon Simple Storage Service (Amazon S3) e conteúdo dinâmico de um balanceador de carga, você pode atender a ambos os tipos de conteúdo de uma distribuição web do Amazon CloudFront.

Use um grupo de origem com origens primárias e secundárias para configurar o Amazon CloudFront para alta disponibilidade e failover

Você pode configurar o Amazon CloudFront com failover de origem para cenários que exigem alta disponibilidade. Para começar, crie um grupo de origem com duas origens: uma primária e uma secundária. Se a origem primária estiver indisponível ou retornar códigos de status de resposta HTTP específicos que indiquem uma falha, o CloudFront alternará automaticamente para a origem

secundária.

Para configurar o failover de origem, você precisa ter uma distribuição com pelo menos duas origens. Em seguida, crie um grupo de origem para sua distribuição que inclua duas origens, definindo uma como primária. Por fim, crie ou atualize um comportamento de cache para usar o grupo de origem.

Use criptografia em nível de campo no Amazon CloudFront para proteger dados confidenciais para conteúdo específico

A criptografia em nível de campo permite que você habilite seus usuários a carregar com segurança informações confidenciais para seus servidores web. As informações confidenciais fornecidas por seus usuários são criptografadas na borda, perto do usuário, e permanecem criptografadas em toda a sua pilha de aplicativos. Essa criptografia garante que apenas os aplicativos que precisam dos dados – e têm as credenciais para descriptografá-los – sejam capazes de fazê-lo.

Para usar a criptografia em nível de campo, ao configurar sua distribuição do Amazon CloudFront, especifique o conjunto de campos em solicitações POST que você deseja criptografar e a chave pública a ser usada para criptografá-los. Você pode criptografar até 10 campos de dados em uma solicitação. (Você não pode criptografar todos os dados em uma solicitação com criptografia em nível de campo; você deve especificar campos individuais para criptografar.)

Pergunta 10

Uma empresa de compartilhamento de viagens quer aprimorar o sistema de rastreamento de viagens que armazena as coordenadas GPS de todas as viagens. A equipe de engenharia da empresa busca um banco de dados NoSQL com latência de um dígito em milissegundos, escalável horizontalmente e sem servidor, para que seja possível realizar consultas de alta frequência com confiabilidade.

Como arquiteto de soluções, qual banco de dados você recomenda para atender às necessidades deles?

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 NoSQL totalmente gerenciado, multirregional, multimestre e durável, com segurança integrada, backup e restauração e cache na memória para aplicativos em escala de internet. O DynamoDB pode processar mais de 10 trilhões de solicitações por dia e suportar picos de mais de 20 milhões de solicitações por segundo. O DynamoDB é serverless, tem latência de milissegundos e escala horizontalmente. Esta é a escolha certa para os requisitos fornecidos.

Pergunta 11

Por motivos de segurança, uma equipe de desenvolvimento decidiu implantar as instâncias do Amazon EC2 em uma sub-rede privada. A equipe planeja usar endpoints VPC para que as instâncias possam acessar alguns serviços da AWS com segurança. Os membros da equipe gostariam de saber mais sobre os dois serviços da AWS que oferecem suporte a endpoints de gateway.

Como arquiteto de soluções, qual dos seguintes serviços você sugeriria para esse requisito? (Selecione dois)

R: Amazon S3

R: Amazon DynamoDB

Opções corretas:

Amazon S3

Amazon DynamoDB

Um endpoint de VPC permite que você conecte sua VPC de forma privada a serviços da AWS compatíveis e a serviços de endpoint de VPC com tecnologia AWS PrivateLink sem a necessidade de um gateway de internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. As instâncias na sua VPC não exigem endereços IP públicos para se comunicar com os recursos no serviço. O tráfego entre a sua VPC e o outro serviço não sai da rede da Amazon.

Endpoints são dispositivos virtuais. São componentes de VPC escalonados horizontalmente, redundantes e altamente disponíveis. Eles permitem a comunicação entre instâncias na sua VPC e serviços sem impor riscos de disponibilidade ou restrições de largura de banda ao tráfego da sua rede.

Existem dois tipos de endpoints de VPC: endpoints de interface e endpoints de gateway. Um endpoint de interface é uma interface de rede elástica com um endereço IP privado do intervalo de endereços IP da sua sub-rede que serve como ponto de entrada para o tráfego destinado a um serviço compatível.

Um endpoint de gateway é um gateway que você especifica como destino de uma rota na sua tabela de rotas para o tráfego destinado a um serviço da AWS compatível. Os seguintes serviços da AWS são compatíveis: Amazon S3 e Amazon DynamoDB. Você pode usar dois tipos de endpoints de VPC para acessar o Amazon S3: endpoints de gateway e endpoints de interface. Um endpoint de gateway é um gateway que você especifica na sua tabela de rotas para acessar o Amazon S3 a partir da sua VPC pela rede AWS. Os endpoints de interface estendem a funcionalidade dos endpoints de gateway usando endereços IP privados para rotear solicitações para o Amazon S3 de dentro da sua VPC, on-premises ou de uma VPC em outra região da AWS usando peering de VPC ou AWS Transit Gateway.

Lembre-se de que esses dois serviços usam um endpoint de gateway VPC. Os demais serviços da AWS usam endpoints de interface VPC.

Pergunta 12

Sua empresa está implantando um site no AWS Elastic Beanstalk. A instalação do site leva mais de 45 minutos e contém arquivos estáticos e dinâmicos que devem ser gerados durante o processo de instalação.

Como Arquiteto de Soluções, você gostaria de reduzir o tempo de criação de uma nova instância na sua implantação do AWS Elastic Beanstalk para menos de 2 minutos. Qual das seguintes opções deve ser combinada para criar uma solução para esse requisito? (Selecione duas)

R: Use os dados do usuário do Amazon EC2 para personalizar as partes da instalação dinâmica no momento da inicialização

R: Crie uma Golden Amazon Machine Image (AMI) com os componentes de instalação estática já configurados

Opções corretas:

O AWS Elastic Beanstalk é um serviço fácil de usar para implantar e dimensionar aplicativos e serviços da Web desenvolvidos com Java, .NET, PHP, Node.js, Python, Ruby, Go e Docker em servidores conhecidos como Apache, Nginx, Passenger e IIS.

Basta fazer o upload do seu código e o Elastic Beanstalk cuidará automaticamente da implantação, desde o provisionamento de capacidade, balanceamento de carga, escalonamento automático até o monitoramento da integridade da aplicação. Ao mesmo tempo, você mantém controle total sobre os recursos da AWS que alimentam sua aplicação e pode acessar os recursos subjacentes a qualquer momento.

Ao criar um ambiente do AWS Elastic Beanstalk, você pode especificar uma Imagem de Máquina da Amazon (AMI) para usar em vez da AMI padrão do Elastic Beanstalk incluída na versão da sua plataforma. Uma AMI personalizada pode melhorar os tempos de provisionamento quando instâncias são iniciadas no seu ambiente, caso você precise instalar muitos softwares que não estão incluídos nas AMIs padrão.

Crie uma Golden Amazon Machine Image (AMI) com os componentes de instalação estática já configurados

- Uma Golden AMI é uma AMI que você padroniza por meio de configuração, aplicação consistente de patches de segurança e reforço. Ela também contém agentes que você aprova para registro em log, segurança, monitoramento de desempenho, etc. Para o caso de uso em questão, você pode ter os componentes de instalação estática já configurados por meio da Golden AMI.

Use os dados do usuário do Amazon EC2 para personalizar as partes da instalação dinâmica no momento da inicialização

- Os dados do usuário da instância do Amazon EC2 são os dados que você especificou na forma de um script de configuração ao iniciar sua instância. Você pode usar os dados do usuário do Amazon EC2 para personalizar as partes da instalação dinâmica na inicialização, em vez de instalar o aplicativo em si.

Pergunta 13

Uma empresa cresceu de uma pequena startup para uma empresa com mais de 1.000 funcionários. À medida que a equipe crescia, a empresa observou recentemente um comportamento estranho, com as configurações dos buckets do Amazon S3 sendo alteradas regularmente.

Como você pode descobrir o que está acontecendo sem restringir os direitos dos usuários?

R: Use o AWS CloudTrail para analisar chamadas de API

Opção correta:

Use o AWS CloudTrail para analisar chamadas de API

O AWS CloudTrail é um serviço que permite a governança, a conformidade, a auditoria operacional e a auditoria de riscos da sua conta da AWS. Com o AWS CloudTrail, você pode registrar, monitorar continuamente e armazenar as atividades da conta relacionadas a ações em toda a sua infraestrutura da AWS. O AWS CloudTrail fornece o histórico de eventos das atividades da sua conta da AWS, incluindo ações realizadas por meio do Console de Gerenciamento da AWS, SDKs da AWS, ferramentas de linha de comando e outros serviços da AWS.

Em geral, o AWS CloudTrail é usado para analisar chamadas de API feitas em uma conta da AWS. Você pode registrar as ações realizadas por usuários, funções ou serviços da AWS em recursos do Amazon S3 e manter registros de log para fins de auditoria e conformidade. Para isso, você pode usar o registro de acesso ao servidor, o registro do AWS CloudTrail ou uma combinação de ambos. A AWS recomenda o uso do AWS CloudTrail para registrar ações em nível de bucket e objeto para seus recursos do Amazon S3.

Pergunta 14

Você está trabalhando como Arquiteto de Soluções para uma empresa de processamento de fotos que tem um algoritmo proprietário para compactar uma imagem sem nenhuma perda de qualidade. Devido à eficiência do algoritmo, seus clientes estão dispostos a esperar por uma resposta que carregue suas imagens compactadas de volta. Você também quer processar esses trabalhos de forma assíncrona e escalar rapidamente, para atender à alta demanda. Além disso, você também quer que o trabalho seja repetido em caso de falhas.

Qual combinação de escolhas você recomenda para minimizar custos e cumprir com os requisitos? (Selecione duas)

R: Serviço de fila simples da Amazon (Amazon SQS)

R: Instâncias Spot do Amazon EC2

Opções corretas:

Instâncias Spot do Amazon EC2

Uma Instância Spot é uma instância não utilizada do Amazon EC2 que está disponível por menos do que o preço On-Demand. Como as Instâncias Spot permitem que você solicite instâncias não utilizadas do Amazon EC2 com grandes descontos, você pode reduzir significativamente seus custos do Amazon EC2. O preço por hora para uma Instância Spot é chamado de preço Spot. O preço Spot de cada tipo de instância em cada Zona de Disponibilidade (AZ) é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e demanda de longo prazo por Instâncias Spot. Sua Instância Spot é executada sempre que a capacidade estiver disponível e o preço máximo por hora para sua solicitação exceder o preço Spot.

Para processar esses trabalhos, devido à natureza imprevisível de seu volume e ao desejo de economizar em custos, as Instâncias spot são recomendadas em comparação às instâncias on-demand. Como as instâncias spot são mais baratas do que as instâncias reservadas e não exigem compromisso

de longo prazo, as instâncias spot são mais adequadas para o caso de uso fornecido.

Serviço de fila simples da Amazon (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 SQS oferece dois tipos de filas de mensagens. As filas padrão oferecem rendimento máximo, ordenação de melhor esforço e entrega pelo menos uma vez. As filas FIFO (First-In-First-out) do Amazon SQS são projetadas para garantir que as mensagens sejam processadas exatamente uma vez, na ordem exata em que são enviadas.

O Amazon SQS permitirá que você armazene em buffer as solicitações de compactação de imagem e as processe de forma assíncrona. Ele também tem um mecanismo direto integrado para novas tentativas e escalas perfeitamente.

Pergunta 15

Um serviço de hospedagem de fotos publica uma coleção de belas imagens de montanhas, todo mês, que agregam mais de 50 gigabytes de tamanho e são baixadas em todo o mundo. O conteúdo está atualmente hospedado no Amazon EFS e distribuído por instâncias do Elastic Load Balancing (ELB) e do Amazon EC2. O site está enfrentando alta carga todo mês e custos de rede muito altos.

Como arquiteto de soluções, o que você pode recomendar que não force uma refatoração de aplicativo e reduza drasticamente os custos de rede e a carga do Amazon EC2?

R: Crie uma distribuição do Amazon CloudFront

Opção correta:

Crie uma distribuição do Amazon CloudFront

O Amazon CloudFront é um serviço rápido de rede de distribuição de conteúdo (CDN) que entrega com segurança dados, vídeos, aplicativos e APIs para clientes em todo o mundo, com baixa latência e altas velocidades de transferência, tudo em um ambiente amigável ao desenvolvedor.

Os pontos de presença (POPs) (localizações de borda) do Amazon CloudFront garantem que conteúdo popular seja disponibilizado rapidamente aos seus espectadores. O Amazon CloudFront também possui caches de borda regionais que aproximam mais do seu conteúdo dos seus espectadores, mesmo quando o conteúdo não é popular o suficiente para permanecer em um POP, ajudando a melhorar o desempenho desse conteúdo.

Os edge caches regionais ajudam com todos os tipos de conteúdo, particularmente conteúdo que tende a se tornar menos popular com o tempo. Exemplos incluem conteúdo gerado pelo usuário, como vídeo, fotos ou arte; ativos de e-commerce, como fotos e vídeos de produtos; e conteúdo relacionado a notícias e eventos que pode repentinamente encontrar nova popularidade.

Para o caso de uso em questão, você precisa criar uma distribuição do Amazon CloudFront para adicionar uma camada de cache antes do seu ELB. Essa camada de cache será muito eficaz, pois o pacote de imagens é um arquivo estático e, portanto, economizaria significativamente os custos de rede sem exigir uma refatoração do aplicativo.

Pergunta 16

Como uma empresa de hospedagem de torneios de e-sport, você tem servidores que precisam ser escalonados e estar altamente disponíveis. Portanto, você implantou um Elastic Load Balancing (ELB) com um grupo de Auto Scaling (ASG) em 3 Availability Zones (AZs). Quando os torneios de e-sport estão em andamento, os servidores precisam ser escalonados rapidamente. E quando os torneios terminam, os servidores podem ficar ociosos. Como regra geral, você gostaria de estar altamente disponível, ter capacidade de escalar e otimizar seus custos.

O que você recomenda? (Selecione duas)

R: Use Instâncias Reservadas (RIs) para a capacidade mínima

R: Defina a capacidade mínima para 2

Opções corretas:

Defina a capacidade mínima para 2

- Um grupo de Auto Scaling contém uma coleção de instâncias do Amazon EC2 que são tratadas como um agrupamento lógico para escalonamento e gerenciamento automáticos. Um grupo de Auto Scaling também permite que você use os recursos do Amazon EC2 Auto Scaling, como substituições de verificações de integridade e políticas de escalonamento. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto o escalonamento automático são as principais funcionalidades do serviço Amazon EC2 Auto Scaling.

Configure o tamanho do seu grupo de Dimensionamento Automático definindo a capacidade mínima, máxima e desejada. As capacidades mínima e máxima são necessárias para criar um grupo de Dimensionamento Automático, enquanto a capacidade desejada é opcional. Se você não definir a capacidade desejada antecipadamente, o padrão será a capacidade mínima.

Um grupo de Dimensionamento Automático é elástico desde que tenha valores diferentes para capacidade mínima e máxima. Todas as solicitações para alterar a capacidade desejada do grupo de Dimensionamento Automático (seja por dimensionamento manual ou automático) devem estar dentro desses limites.

Aqui, embora nosso ASG esteja implantado em 3 Zonas de Disponibilidade (AZs), a capacidade mínima para alta disponibilidade é 2. Quando especificamos 2 como capacidade mínima, o ASG criaria essas 2 instâncias em Zonas de Disponibilidade (AZs) separadas. Se a demanda aumentar, o ASG criaria uma nova instância na terceira Zona de Disponibilidade (AZ). Posteriormente, à medida que a demanda diminuir, o ASG será dimensionado horizontalmente e a contagem de instâncias voltará para 2.

Use Instâncias Reservadas (RIs) para a capacidade mínima

- As Instâncias Reservadas (RIs) proporcionam economias significativas nos custos do Amazon EC2 em comparação com o preço das Instâncias Sob Demanda. Instâncias Reservadas não são instâncias físicas, mas sim um desconto de faturamento aplicado ao uso de Instâncias Sob Demanda na sua conta. Essas Instâncias Sob Demanda devem atender a determinados atributos, como tipo de instância e região, para se beneficiarem do desconto de faturamento. Como a capacidade mínima será sempre mantida, é mais econômico optar por instâncias reservadas do que por qualquer outra opção.

Em caso de interrupção da Availability Zone (AZ), a instância naquela Availability Zone (AZ) ficaria inativa, mas a outra instância ainda estaria disponível. O ASG provisionaria a instância de substituição na terceira Availability Zone (AZ) para manter a contagem mínima em 2.

Pergunta 17

Uma empresa farmacêutica está procurando uma solução simples para conectar suas VPCs e redes locais por meio de um hub central.

Como arquiteto de soluções, qual das seguintes opções você sugeriria como a solução que requer MENOR sobrecarga operacional?

R: Use o AWS Transit Gateway para conectar as Amazon VPCs às redes locais

Opção correta:

Use o AWS Transit Gateway para conectar as Amazon VPCs às redes locais

O AWS Transit Gateway permite que os clientes conectem suas Amazon VPCs e suas redes locais a um único gateway. À medida que o número de cargas de trabalho em execução na AWS aumenta, você precisa escalar suas redes entre várias contas e Amazon VPCs para acompanhar o crescimento. Com o AWS Transit Gateway, você só precisa criar e gerenciar uma única conexão do gateway central para cada Amazon VPC, data center local ou escritório remoto em sua rede. O AWS Transit Gateway atua como um hub que controla como o tráfego é roteado entre todas as redes conectadas, que funcionam como spokes. Esse modelo de hub e spoke simplifica o gerenciamento e reduz os custos operacionais, pois cada rede precisa se conectar apenas ao Transit Gateway e não a todas as outras redes.

Gateway de trânsito da AWS:

Pergunta 18

Um administrador de sistemas está criando políticas do IAM e anexando-as às identidades do IAM. Após criar as políticas baseadas em identidade necessárias, o administrador agora cria políticas baseadas em recursos.

Qual é a única política baseada em recursos suportada pelo serviço IAM?

R: Política de confiança

Opção correta:

Você gerencia o acesso na AWS criando políticas e anexando-as a identidades do IAM (usuários, grupos de usuários ou funções) ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. Políticas baseadas em recursos são documentos de política JSON que você anexa a um recurso, como um bucket do Amazon S3. Essas políticas concedem à entidade especificada a permissão para executar ações específicas nesse recurso e definem em que condições isso se aplica.

Política de confiança

- As políticas de confiança definem quais entidades principais (contas, usuários, funções e usuários federados) podem assumir a função. Uma função do IAM é tanto uma identidade quanto um recurso que oferece suporte a políticas baseadas em recursos. Por esse motivo, você deve anexar uma política de confiança e uma política baseada em identidade a uma função do IAM. O serviço do IAM oferece suporte a apenas um tipo de política baseada em recursos, chamada política de confiança de função, que é anexada a uma função do IAM.

Pergunta 19

Uma empresa migrou seu aplicativo de uma arquitetura monolítica para uma arquitetura baseada em microsserviços. A equipe de desenvolvimento atualizou o registro simples do Amazon Route 53 para apontar "myapp.mydomain.com" do antigo Load Balancer para o novo.

Os usuários ainda não são redirecionados para o novo Load Balancer. O que deu errado na configuração?

R: O Time To Live (TTL) ainda está em vigor

Opção correta:

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, balanceadores de carga do Elastic Load Balancing ou buckets do Amazon S3 – e também pode ser usado para rotear usuários para infraestruturas fora da AWS. Você pode usar o Amazon Route 53 para configurar verificações de integridade de DNS para rotear o tráfego para endpoints íntegros ou monitorar de forma independente a integridade do seu aplicativo e de seus endpoints. O Amazon Route 53 Traffic Flow facilita o gerenciamento global do tráfego por meio de diversos tipos de roteamento, incluindo Roteamento Baseado em Latência, Geo DNS, Geoproximity e Weighted Round Robin – todos os quais podem ser combinados com o Failover de DNS para habilitar uma variedade de arquiteturas de baixa latência e tolerantes a falhas.

O Time To Live (TTL) ainda está em vigor

TTL (time to live) é a quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem em cache informações sobre um registro. Se você especificar um valor maior (por exemplo, 172800 segundos ou dois dias), você reduz o número de chamadas que os resolvedores recursivos de DNS devem fazer para o Amazon Route 53 para obter as informações mais recentes do registro. Isso tem o efeito de reduzir a latência e reduzir sua conta pelo serviço Route 53.

No entanto, se você especificar um valor maior para o TTL, as alterações no registro (por exemplo, um novo endereço IP) levarão mais tempo para entrar em vigor, pois os resolvedores recursivos usam

os valores em seu cache por períodos mais longos antes de solicitarem as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio já em uso, a AWS recomenda que você especifique inicialmente um valor menor, como 300 segundos, e aumente o valor após confirmar que as novas configurações estão corretas.

Para este caso de uso, o problema mais provável é que o TTL ainda esteja em vigor, então você terá que esperar até que ele expire para que a nova solicitação execute outra consulta DNS e obtenha o valor para o novo balanceador de carga.

Pergunta 20

Uma empresa deseja adotar uma infraestrutura de nuvem híbrida, utilizando alguns serviços da AWS, como o Amazon S3, juntamente com seu data center local. A empresa deseja uma conexão privada dedicada entre o data center local e a AWS. Em caso de falhas, porém, a empresa precisa garantir o tempo de atividade e está disposta a usar a internet pública para uma conexão criptografada.

O que você recomenda? (Selecione duas)

R: Use a conexão AWS Direct Connect como conexão primária

R: Use o AWS Site-to-Site VPN como uma conexão de backup

Opções corretas:

Use a conexão AWS Direct Connect como conexão primária

- O AWS Direct Connect permite que você estabeleça uma conexão de rede dedicada entre sua rede e um dos locais do AWS Direct Connect. Utilizando VLANs 802.1q padrão do setor, essa conexão dedicada pode ser particionada em várias interfaces virtuais. O AWS Direct Connect não envolve a internet; em vez disso, ele usa conexões de rede privadas dedicadas entre sua intranet e a Amazon VPC.

Use o AWS Site-to-Site VPN como uma conexão de backup

A VPN Site-to-Site da AWS permite que você conecte com segurança sua rede local ou filial à sua Amazon Virtual Private Cloud (Amazon VPC). Você pode estender com segurança a rede do seu data center ou filial para a nuvem com uma conexão VPN Site-to-Site da AWS. Uma conexão VPN VPC utiliza IPsec para estabelecer conectividade de rede criptografada entre sua intranet e a Amazon VPC pela internet. As conexões VPN podem ser configuradas em minutos e são uma boa solução se você tiver uma necessidade imediata, requisitos de largura de banda baixos e modestos e puder tolerar a variabilidade inerente à conectividade baseada na internet.

O AWS Direct Connect como conexão primária garante ótimo desempenho e segurança (já que a conexão é privada). Usar o Direct Connect como solução de backup funcionaria, mas provavelmente também corre o risco de falhar. Como não nos importamos em usar a internet pública (que é confiável, mas menos segura, já que as conexões são feitas por via pública), devemos usar uma VPN Site to Site que ofereça uma conexão criptografada para lidar com cenários de failover.

Pergunta 21

A infraestrutura de nuvem de uma startup consiste em algumas instâncias do Amazon EC2, instâncias do Amazon RDS e armazenamento no Amazon S3. Após um ano de operação, a startup está incorrendo em custos que parecem altos demais para suas necessidades comerciais.

Qual das seguintes opções representa uma solução válida de otimização de custos?

R: Use o AWS Cost Explorer Resource Optimization para obter um relatório de instâncias do Amazon EC2 que estão ociosas ou com baixa utilização e use o AWS Compute Optimizer para analisar recomendações de tipo de instância.

Opção correta:

Use o AWS Cost Explorer Resource Optimization para obter um relatório de instâncias do Amazon EC2 que estão ociosas ou com baixa utilização e use o AWS Compute Optimizer para analisar recomendações de tipo de instância.

O AWS Cost Explorer ajuda você a identificar instâncias subutilizadas do Amazon EC2 que podem ser reduzidas instância por instância dentro da mesma família de instâncias, além de entender o impacto

potencial na sua fatura da AWS levando em consideração suas Instâncias Reservadas e Planos de Economia.

O AWS Compute Optimizer recomenda os recursos ideais do AWS Compute para suas cargas de trabalho, a fim de reduzir custos e melhorar o desempenho usando aprendizado de máquina para analisar métricas históricas de utilização. O Compute Optimizer ajuda você a escolher os tipos ideais de instância do Amazon EC2, incluindo aquelas que fazem parte de um grupo de Auto Scaling do Amazon EC2, com base nos seus dados de utilização.

Pergunta 22

Uma empresa de Internet das Coisas (IoT) gostaria de ter um sistema de streaming que realizasse análises em tempo real dos dados de IoT ingeridos. Após a conclusão das análises, a empresa gostaria de enviar notificações para os aplicativos móveis dos proprietários dos dispositivos de IoT.

Como arquiteto de soluções, qual das seguintes tecnologias da AWS você recomendaria para enviar essas notificações aos aplicativos móveis?

R: Amazon Kinesis com Amazon Simple Notification Service (Amazon SNS)

Opção correta:

Amazon Kinesis com Amazon Simple Notification Service (Amazon SNS)

O Amazon Kinesis facilita a coleta, o processamento e a análise de dados de streaming em tempo real para que você possa obter insights oportunos e reagir rapidamente a novas informações. O Amazon Kinesis oferece recursos essenciais para processar dados de streaming de forma econômica em qualquer escala, juntamente com a flexibilidade de escolher as ferramentas que melhor atendem aos requisitos do seu aplicativo.

Com o Amazon Kinesis, você pode ingerir dados em tempo real, como vídeo, áudio, logs de aplicativos, fluxos de cliques de sites e dados de telemetria de IoT para aprendizado de máquina, análises e outros aplicativos. O Amazon Kinesis permite que você processe e analise dados conforme eles chegam e responda instantaneamente em vez de ter que esperar até que todos os seus dados sejam coletados antes que o processamento possa começar.

O Amazon Kinesis será ótimo para streaming de eventos de dispositivos IoT, mas não para enviar notificações, pois não tem esse recurso.

O Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens pub/sub altamente disponível, durável, seguro e totalmente gerenciado que permite desacoplar microsserviços, sistemas distribuídos e aplicativos sem servidor. O Amazon SNS fornece tópicos para mensagens de alto rendimento, baseadas em push e muitos para muitos. O Amazon SNS é um serviço de notificação e será perfeito para esse caso de uso.

Transmitir dados com o Amazon Kinesis e usar o Amazon SNS para enviar notificações de resposta é a solução ideal para o cenário atual.

Pergunta 23

Uma empresa de varejo utiliza a Nuvem AWS para gerenciar sua infraestrutura tecnológica. A empresa implantou seu aplicativo web voltado para o consumidor em servidores web baseados no Amazon EC2 e utiliza o banco de dados PostgreSQL do Amazon RDS como armazenamento de dados. O banco de dados PostgreSQL está configurado em uma sub-rede privada que permite tráfego de entrada de instâncias selecionadas do Amazon EC2. O banco de dados também utiliza o AWS Key Management Service (AWS KMS) para criptografar dados em repouso.

Qual das seguintes etapas você recomendaria para facilitar a segurança de ponta a ponta dos dados em trânsito ao acessar o banco de dados?

R: Configurar o Amazon RDS para usar SSL para dados em trânsito

Opção correta:

Configurar o Amazon RDS para usar SSL para dados em trânsito

Você pode usar conexões Secure Socket Layer/Transport Layer Security (SSL/TLS) para criptografar dados em trânsito. O Amazon RDS cria um certificado SSL e instala o certificado na instância do BD quando a instância é provisionada. Para MySQL, você inicia o cliente MySQL usando o parâmetro `--ssl_ca` para referenciar a chave pública para criptografar conexões. Usando SSL, você pode criptografar uma conexão PostgreSQL entre seus aplicativos e suas instâncias de BD PostgreSQL. Você também pode forçar todas as conexões com sua instância de BD PostgreSQL a usar SSL.

Pergunta 24

Um desenvolvedor em sua empresa configurou uma arquitetura clássica de 2 camadas que consiste em um Application Load Balancer e um grupo de Auto Scaling (ASG) gerenciando uma frota de instâncias do Amazon EC2. O Application Load Balancer é implantado em uma sub-rede de tamanho `10.0.1.0/24` e o grupo de Auto Scaling é implantado em uma sub-rede de tamanho `10.0.4.0/22`.

Como arquiteto de soluções, você gostaria de aderir ao pilar de segurança do framework bem-arquitetado. Como você configura o grupo de segurança das instâncias do Amazon EC2 para permitir apenas tráfego vindo do Application Load Balancer?

R: Adicione uma regra para autorizar o grupo de segurança do Application Load Balancer

Opção correta:

Um grupo de Auto Scaling (ASG) contém uma coleção de instâncias do Amazon EC2 que são tratadas como um agrupamento lógico para dimensionamento e gerenciamento automáticos. Um grupo de Auto Scaling também permite que você use os recursos do Amazon EC2 Auto Scaling, como substituições de verificação de integridade e políticas de dimensionamento. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto o dimensionamento automático são a funcionalidade principal do serviço Amazon EC2 Auto Scaling.

Adicione uma regra para autorizar o grupo de segurança do Application Load Balancer

- 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, usaremos 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. Ao decidir permitir que o tráfego chegue a uma instância, todas as regras de todos os grupos de segurança associados a ela são avaliadas.

As seguintes são as características das regras de grupo de segurança: 1. Por padrão, os grupos de segurança permitem todo o tráfego de saída. 2. As regras de grupo de segurança são sempre permissivas; você não pode criar regras que neguem acesso. 3. Os grupos de segurança são com estado. O Application Load Balancer (ALB) opera no nível de solicitação (camada 7), roteando tráfego para alvos - instâncias do Amazon EC2, contêineres, endereços IP e funções Lambda com base no conteúdo da solicitação. Ideal para balanceamento de carga avançado de tráfego HTTP e HTTPS, o Application Load Balancer fornece roteamento de solicitação avançado direcionado à entrega de arquiteturas de aplicativos modernos, incluindo microsserviços e aplicativos baseados em contêiner.

Pergunta 25

Uma empresa de mídia usa o Amazon ElastiCache Redis para melhorar o desempenho de sua camada de banco de dados Amazon RDS. A empresa quer uma estratégia de recuperação de desastres robusta para sua camada de cache que garanta tempo de inatividade mínimo, bem como perda mínima de dados, ao mesmo tempo em que garante um bom desempenho do aplicativo.

Qual das seguintes soluções você recomendaria para abordar o caso de uso fornecido?

R: Opção pela configuração Multi-AZ com funcionalidade de failover automático para ajudar a mitigar falhas

Opção correta:

Opção pela configuração Multi-AZ com funcionalidade de failover automático para ajudar a mitigar falhas

Multi-AZ é a melhor opção quando a retenção de dados, o tempo de inatividade mínimo e o desempenho do aplicativo são prioridades.

Potencial de perda de dados - Baixo. O Multi-AZ fornece tolerância a falhas para todos os cenários, incluindo problemas relacionados a hardware.

Impacto no desempenho - Baixo. Das opções disponíveis, o Multi-AZ fornece o tempo mais rápido para recuperação, porque não há um procedimento manual a ser seguido após o processo ser implementado.

Custo - De baixo a alto. Multi-AZ é a opção de menor custo. Use Multi-AZ quando não puder arriscar perder dados devido a falha de hardware ou não puder arcar com o tempo de inatividade exigido por outras opções em sua resposta a uma interrupção.

Pergunta 26

Uma empresa de mídia digital precisa gerenciar uploads de cerca de 1 terabyte cada, de um aplicativo usado por uma empresa parceira.

Como arquiteto de soluções, como você lidará com o upload desses arquivos para o Amazon S3?

R: Use o recurso de upload multiparte do Amazon S3

Opção correta:

Use o recurso de upload multiparte do Amazon S3

O upload multiparte permite que você carregue um único objeto como um conjunto de partes. Cada parte é uma porção contígua dos dados do objeto. Você pode carregar essas partes do objeto independentemente e em qualquer ordem. Se a transmissão de qualquer parte falhar, você pode retransmitir essa parte sem afetar outras partes. Depois que todas as partes do seu objeto forem carregadas, o Amazon S3 monta essas partes e cria o objeto.

A AWS recomenda que você use o upload multiparte das seguintes maneiras: 1. Se você estiver carregando objetos grandes em uma rede estável de alta largura de banda, use o upload multiparte para maximizar o uso da sua largura de banda disponível carregando partes do objeto em paralelo para desempenho multithread. 2. Se você estiver carregando em uma rede irregular, use o upload multiparte para aumentar a resiliência a erros de rede evitando reinicializações de upload. Ao usar o upload multiparte, você precisa tentar carregar novamente apenas as partes que são interrompidas durante o upload. Você não precisa reiniciar o upload do seu objeto desde o início.

Em geral, quando o tamanho do seu objeto atinge 100 megabytes, você deve considerar usar multipart uploads em vez de carregar o objeto em uma única operação. Se o arquivo for maior que 5 gigabytes, você deve usar multi-part upload para carregar esse arquivo no Amazon S3.

Pergunta 27

Uma empresa administra um site de namoro popular na Nuvem AWS. Como Arquiteto de Soluções, você projetou a arquitetura do site para seguir um padrão sem servidor na Nuvem AWS usando o Amazon API Gateway e o AWS Lambda. O backend usa um banco de dados Amazon RDS PostgreSQL. Atualmente, o aplicativo usa uma combinação de nome de usuário e senha para conectar a função AWS Lambda ao banco de dados Amazon RDS.

Você gostaria de melhorar a segurança no nível de autenticação alavancando credenciais de curta duração. O que você escolherá? (Selecione duas)

Seleção correta

R: Anexar uma função AWS Identity and Access Management (IAM) ao AWS Lambda

R: Use a autenticação IAM do AWS Lambda para o Amazon RDS PostgreSQL

Opções corretas:

Use a autenticação IAM do AWS Lambda para o Amazon RDS PostgreSQL

Anexar uma função AWS Identity and Access Management (IAM) ao AWS Lambda

Você pode autenticar sua instância de banco de dados usando a autenticação de banco de dados do AWS Identity and Access Management (IAM). A autenticação de banco de dados do IAM funciona com MySQL e PostgreSQL. Com esse método de autenticação, você não precisa usar uma senha ao se conectar a uma instância de banco de dados. Em vez disso, você usa um token de autenticação.

Um token de autenticação é uma sequência exclusiva de caracteres que o Amazon RDS gera mediante solicitação. Os tokens de autenticação são gerados usando o AWS Signature versão 4. Cada token tem uma vida útil de 15 minutos. Você não precisa armazenar credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente usando o IAM. Você também pode usar a autenticação de banco de dados padrão.

A autenticação do banco de dados do IAM fornece os seguintes benefícios: 1. O tráfego de rede de e para o banco de dados é criptografado usando Secure Sockets Layer (SSL). 2. Você pode usar o IAM para gerenciar centralmente o acesso aos recursos do seu banco de dados, em vez de gerenciar o acesso individualmente em cada instância do banco de dados. 3. Para aplicativos em execução no Amazon EC2, você pode usar credenciais de perfil específicas para sua instância do Amazon EC2 para acessar seu banco de dados em vez de uma senha, para maior segurança.

Pergunta 28

Uma empresa de e-commerce deseja migrar sua aplicação local para a AWS. A aplicação consiste em servidores de aplicação e um banco de dados Microsoft SQL Server. A solução deve resultar na máxima disponibilidade possível para a camada de banco de dados, minimizando a sobrecarga operacional e de gerenciamento.

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

R: Migrar os dados para o Amazon RDS para banco de dados SQL Server em uma implantação Multi-AZ

Opção correta:

Migrar os dados para o Amazon RDS para banco de dados SQL Server em uma implantação Multi-AZ

O Amazon RDS oferece suporte a implantações Multi-AZ para o Microsoft SQL Server usando o Espelhamento de Banco de Dados (DBM) do SQL Server ou Grupos de Disponibilidade (AGs) Always On. O Amazon RDS monitora e mantém a integridade da sua implantação Multi-AZ. Em caso de problemas, o Amazon RDS repara automaticamente instâncias de banco de dados com problemas, restabelece a sincronização e inicia failovers.

Implantações Multi-AZ proporcionam maior disponibilidade, durabilidade dos dados e tolerância a falhas para instâncias de banco de dados. Em caso de manutenção planejada do banco de dados ou interrupção não planejada do serviço, o Amazon RDS realiza o failover automaticamente para a instância secundária atualizada do banco de dados. Essa funcionalidade permite que as operações do banco de dados sejam retomadas rapidamente, sem intervenção manual. As instâncias primária e em espera usam o mesmo endpoint, cujo endereço de rede física transita para a réplica secundária como parte do processo de failover. Você não precisa reconfigurar seu aplicativo quando ocorre um failover.

Esta opção fornece a máxima disponibilidade possível para a camada de banco de dados, minimizando a sobrecarga operacional e de gerenciamento.

Pergunta 29

Uma empresa usa Application Load Balancers em várias regiões da AWS. Os Application Load Balancers recebem tráfego inconsistente que varia ao longo do ano. A equipe de engenharia da empresa precisa permitir os endereços IP dos Application Load Balancers no firewall local para habilitar a conectividade.

Qual das seguintes opções representa a solução MAIS escalável com alterações mínimas de configuração?

R: Configure o AWS Global Accelerator. Registre os Application Load Balancers em diferentes regiões no AWS Global Accelerator. Configure a regra do firewall local para permitir endereços IP estáticos associados ao AWS Global Accelerator

Opção correta:

Configure o AWS Global Accelerator. Registre os Application Load Balancers em diferentes regiões no AWS Global Accelerator. Configure a regra do firewall local para permitir endereços IP estáticos associados ao AWS Global Accelerator

O AWS Global Accelerator é um serviço de rede que ajuda você 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 da AWS.

Associe os endereços IP estáticos fornecidos pelo AWS Global Accelerator a recursos ou endpoints regionais da AWS, como Network Load Balancers, Application Load Balancers, Amazon EC2 Instances e endereços Elastic IP. Os endereços IP são anycast de locais de borda da AWS, de modo que eles fornecem integração à rede global da AWS perto de seus usuários.

Pergunta 30

A equipe de engenharia de uma empresa líder em comércio eletrônico está prevendo um aumento no tráfego por causa de uma venda relâmpago planejada para o fim de semana. Você estimou que o tráfego da web é 10x. O conteúdo do seu site é altamente dinâmico e muda com muita frequência.

Como arquiteto de soluções, qual das seguintes opções você recomendaria para garantir que sua infraestrutura seja dimensionada para esse dia?

R: Use um grupo de dimensionamento automático

Opção correta:

Use um grupo de dimensionamento automático

Um grupo de Auto Scaling (ASG) contém uma coleção de instâncias do Amazon EC2 que são tratadas como um agrupamento lógico para dimensionamento e gerenciamento automáticos. Um grupo de Auto Scaling também permite que você use os recursos do Amazon EC2 Auto Scaling, como substituições de verificação de integridade e políticas de dimensionamento. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto o dimensionamento automático são a funcionalidade principal do serviço Amazon EC2 Auto Scaling.

O tamanho de um grupo de Auto Scaling depende do número de instâncias que você define como a capacidade desejada. Você pode ajustar seu tamanho para atender à demanda, manualmente ou usando o dimensionamento automático.

Um grupo de Auto Scaling começa iniciando instâncias suficientes para atender à capacidade desejada. Ele mantém esse número de instâncias executando verificações periódicas de integridade nas instâncias do grupo. O grupo de Auto Scaling continua a manter um número fixo de instâncias, mesmo se uma instância se tornar não íntegra. Se uma instância se tornar não íntegra, o grupo encerra a instância não íntegra e inicia outra instância para substituí-la.

O grupo de dimensionamento automático é a resposta correta aqui.

Pergunta 31

Uma empresa de jogos para dispositivos móveis está enfrentando um tráfego intenso de leitura em seu banco de dados Amazon Relational Database Service (Amazon RDS), que recupera pontuações e estatísticas dos jogadores. A empresa está usando um tipo de instância de banco de dados Amazon RDS que não é econômico para seu orçamento. A empresa gostaria de implementar uma estratégia para lidar com o alto volume de tráfego de leitura, reduzir a latência e também reduzir o tamanho da instância para reduzir custos.

Qual das seguintes soluções você recomenda?

R: Configurar o Amazon ElastiCache antes do Amazon RDS

Opção correta:

Configurar o Amazon ElastiCache antes do Amazon RDS

O Amazon ElastiCache é um front-end ideal para armazenamentos de dados como o Amazon RDS, fornecendo uma camada intermediária de alto desempenho para aplicações com taxas de solicitação extremamente altas e/ou requisitos de baixa latência. A melhor parte do cache é que ele é minimamente invasivo de implementar e, assim, o desempenho da sua aplicação, tanto em escala quanto em velocidade, é drasticamente aprimorado.

Pergunta 32

Uma empresa deseja conceder acesso a um bucket do Amazon S3 a usuários de sua própria conta na AWS, bem como a usuários de outra conta na AWS. Qual das seguintes opções pode ser usada para atender a esse requisito?

R: Use uma política de bucket para conceder permissão aos usuários em sua conta, bem como aos usuários em outra conta

Opção correta:

Use uma política de bucket para conceder permissão aos usuários em sua conta, bem como aos usuários em outra conta

Uma política de bucket é um tipo de política baseada em recursos que pode ser usada para conceder permissões ao principal especificado na política. Os principais podem estar na mesma conta que o recurso ou em outras contas. Para permissões entre contas para outras contas da AWS ou usuários em outra conta, você deve usar uma política de bucket.

Pergunta 33

A equipe de engenharia de uma empresa global de e-commerce está revisando sua estratégia de recuperação de desastres. A equipe definiu que precisa recuperar rapidamente sua pilha de aplicativos com um Objetivo de Tempo de Recuperação (RTO) de 5 minutos, em todas as regiões da AWS em que o aplicativo é executado. Atualmente, a pilha de aplicativos leva mais de 45 minutos para ser instalada em um sistema Linux.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como estratégia de recuperação de desastres?

R: Crie uma Imagem de Máquina da Amazon (AMI) após instalar o software e copie a AMI para todas as regiões. Use esta AMI específica da região para executar o processo de recuperação nas respectivas regiões.

Opção correta:

Crie uma Imagem de Máquina da Amazon (AMI) após instalar o software e copie a AMI para todas as regiões. Use esta AMI específica da região para executar o processo de recuperação nas respectivas regiões.

Uma Imagem de Máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. Você deve especificar uma AMI ao iniciar uma instância. Você pode iniciar várias instâncias a partir de uma única AMI quando precisar de várias instâncias com a mesma configuração. Você pode usar AMIs diferentes para iniciar instâncias quando precisar de instâncias com configurações diferentes. Para o caso de uso atual, você precisa criar uma AMI de forma que a pilha de aplicativos já esteja configurada. Mas as AMIs estão vinculadas à região em que são criadas. Portanto, você precisa copiar a AMI entre regiões para garantir a preparação para recuperação de desastres.

Copiar uma AMI de origem resulta em uma AMI de destino idêntica, porém distinta, com seu próprio identificador exclusivo. No caso de uma AMI com suporte do Amazon EBS, cada um de seus snapshots de suporte é, por padrão, copiado para um snapshot de destino idêntico, porém distinto. (As únicas exceções são quando você opta por criptografar ou recriptografar o snapshot.) Você pode alterar ou cancelar o registro da AMI de origem sem afetar a AMI de destino. O inverso também é verdadeiro. Não há custos para copiar uma AMI. No entanto, aplicam-se as taxas padrão de armazenamento e

transferência de dados. Se você copiar uma AMI com suporte do Amazon EBS, serão cobradas taxas pelo armazenamento de quaisquer snapshots adicionais do Amazon EBS.

A AWS não copia permissões de inicialização, tags definidas pelo usuário ou permissões de bucket do Amazon S3 da AMI de origem para a nova AMI. Após a conclusão da operação de cópia, você poderá aplicar permissões de inicialização, tags definidas pelo usuário e permissões de bucket do Amazon S3 à nova AMI.

Pergunta 34

Como parte da migração do data center local para a Nuvem AWS, uma empresa está pensando em usar vários dispositivos da família AWS Snow para mover seus dados locais.

Qual serviço da família AWS Snow oferece o recurso de clustering de armazenamento?

R: AWS Snowball Edge otimizado para computação

Opção correta:

AWS Snowball Edge otimizado para computação

O AWS Snowball é um dispositivo de migração de dados e edge computing que vem em duas opções de dispositivo: Compute Optimized e Storage Optimized. Os dispositivos AWS Snowball Edge Storage Optimized fornecem 40 vCPUs de capacidade de computação juntamente com 80 terabytes de armazenamento de bloco ou objeto compatível com Amazon S3 utilizável. Ele é bem adequado para armazenamento local e transferência de dados em larga escala. Os dispositivos AWS Snowball Edge Compute Optimized fornecem 52 vCPUs, 42 terabytes de armazenamento de bloco ou objeto utilizável e uma GPU opcional para casos de uso como aprendizado de máquina avançado e análise de vídeo em movimento completo em ambientes desconectados.

Os clientes podem usar essas duas opções para coleta de dados, aprendizado de máquina e processamento, e armazenamento em ambientes com conectividade intermitente (como manufatura, indústria e transporte) ou em locais extremamente remotos (como operações militares ou marítimas) antes de enviá-los de volta para a AWS. Esses dispositivos também podem ser montados em rack e agrupados para construir instalações maiores e temporárias.

Portanto, tanto o AWS Snowball Edge Storage Optimized quanto o AWS Snowball Edge Compute Optimized oferecem o recurso de cluster de armazenamento.

Pergunta 35

Sua empresa administra um portal da web para conectar desenvolvedores a clientes que precisam de ajuda. Como arquiteto de soluções, você projetou a arquitetura do site para ser totalmente serverless com Amazon API Gateway e AWS Lambda. O backend usa a tabela Amazon DynamoDB. Você gostaria de parabenizar automaticamente seus desenvolvedores por marcos importantes, como - seu primeiro contrato pago. Todos os contratos são armazenados no Amazon DynamoDB.

Qual recurso do Amazon DynamoDB você pode usar para implementar essa funcionalidade de forma que haja MENOR atraso no envio de notificações automáticas?

R: Fluxos do Amazon DynamoDB + AWS Lambda

Opção correta:

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 aplicações em escala de internet.

Fluxos do Amazon DynamoDB + AWS Lambda

O fluxo do Amazon DynamoDB é um fluxo ordenado de informações sobre alterações em itens na tabela do Amazon DynamoDB. Quando você habilita um fluxo em uma tabela, o DynamoDB captura informações sobre cada modificação em itens de dados na tabela. Sempre que um aplicativo cria, atualiza ou exclui itens na tabela, o DynamoDB Streams grava um registro de fluxo com os atributos de chave

primária dos itens que foram modificados. Um registro de fluxo contém informações sobre uma modificação de dados em um único item em uma tabela do DynamoDB.

O Amazon DynamoDB Streams conterá um fluxo de todas as alterações que acontecem em uma tabela do Amazon DynamoDB. Ele pode ser encadeado com uma função do AWS Lambda que será acionada para reagir a essas alterações, uma das quais é o marco do desenvolvedor. Portanto, esta é a opção correta.

Pergunta 36

Uma empresa criou recentemente um novo departamento para lidar com sua carga de trabalho de serviços. Uma equipe de TI foi solicitada a criar uma VPC personalizada para isolar os recursos criados neste novo departamento. Eles configuraram a sub-rede pública e o gateway de internet (IGW). No entanto, eles não conseguem fazer ping nas instâncias do Amazon EC2 com endereço IP elástico (EIP) lançado na VPC recém-criada.

Como um Solution Architect, a equipe solicitou sua ajuda. Como você solucionará esse cenário? (Selecione duas)

R: Verifique se a tabela de rotas está configurada com gateway de internet

R: Verifique se os grupos de segurança permitem ping da fonte

Opções corretas:

Verifique se a tabela de rotas está configurada com gateway de internet

- Um gateway de internet (IGW) é um componente VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre instâncias em sua VPC e a internet. Um gateway de internet serve a dois propósitos: fornecer um alvo em suas tabelas de rotas de VPC para tráfego roteável pela internet e executar a tradução de endereços de rede (NAT) para instâncias que receberam endereços IPv4 públicos. Um gateway de internet suporta tráfego IPv4 e IPv6.

Para habilitar o acesso de ou para a Internet para instâncias em uma sub-rede em uma VPC, você deve fazer o seguinte: 1. Anexe um gateway de Internet à sua VPC. 2. Adicione uma rota à tabela de rotas da sua sub-rede que direcione o tráfego vinculado à Internet para o gateway de Internet. 3. Certifique-se de que as instâncias na sua sub-rede tenham um endereço IP globalmente exclusivo. 4. 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.

Uma tabela de rotas contém um conjunto de regras, chamadas rotas, que são usadas para determinar para onde o tráfego de rede da sua sub-rede ou gateway é direcionado. Após criar um IGW, certifique-se de que as tabelas de rotas estejam atualizadas. Além disso, certifique-se de que o grupo de segurança permita o protocolo ICMP para solicitações de ping.

Verifique se os grupos de segurança permitem ping da fonte

- Um grupo de segurança atua como um firewall virtual que controla o tráfego para uma ou mais instâncias. Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança; caso contrário, a AWS usa o grupo de segurança padrão. Você pode adicionar regras a cada grupo de segurança que permitam tráfego de ou para suas instâncias associadas. Você pode modificar as regras para um grupo de segurança a qualquer momento; as novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança. Para decidir se deve permitir que o tráfego alcance uma instância, todas as regras de todos os grupos de segurança associados à instância são avaliadas.

As seguintes são as características das regras de grupo de segurança: 1. Por padrão, os grupos de segurança permitem todo o tráfego de saída. 2. As regras de grupo de segurança são sempre permissivas; você não pode criar regras que neguem acesso. 3. Os grupos de segurança são com estado

Pergunta 37

Uma empresa de TI tem um grande número de clientes optando por construir sua interface de programação de aplicativos (API) usando contêineres Docker. Para facilitar a hospedagem desses

contêineres, a empresa está analisando vários serviços de orquestração disponíveis com a AWS.

Como Arquiteto de Soluções, qual das seguintes soluções você sugeriria? (Selecione duas)

Seleção correta

R: Use o Amazon Elastic Kubernetes Service (Amazon EKS) com o AWS Fargate para orquestração sem servidor dos serviços em contêineres

R: Use o Amazon Elastic Container Service (Amazon ECS) com o AWS Fargate para orquestração sem servidor dos serviços em contêineres

Opções corretas:

Use o Amazon Elastic Kubernetes Service (Amazon EKS) com o AWS Fargate para orquestração sem servidor dos serviços em contêineres

Use o Amazon Elastic Container Service (Amazon ECS) com o AWS Fargate para orquestração sem servidor dos serviços em contêineres

A construção de APIs com contêineres Docker vem ganhando força ao longo dos anos. Para hospedar e expor essas APIs baseadas em contêineres, elas precisam de uma solução que suporte roteamento de solicitações HTTP, dimensionamento automático e alta disponibilidade. Em alguns casos, a autorização do usuário também é necessária. Para esse propósito, muitas organizações estão orquestrando seus serviços em contêineres com o Amazon Elastic Container Service (Amazon ECS) ou o Amazon Elastic Kubernetes Service (Amazon EKS), enquanto hospedam seus contêineres no Amazon EC2 ou AWS Fargate. Então, elas podem adicionar escalabilidade e alta disponibilidade com o Service Auto Scaling (no Amazon ECS) ou o Horizontal Pod Auto Scaler (no Amazon EKS), e expõem os serviços por meio de balanceadores de carga.

Ao usar o Amazon ECS como um orquestrador (com o tipo de inicialização EC2 ou Fargate), você também tem a opção de expor seus serviços com o Amazon API Gateway e o AWS Cloud Map em vez de um balanceador de carga. O AWS Cloud Map é usado para descoberta de serviços: não importa como as tarefas do Amazon ECS escalam, os nomes de serviço do AWS Cloud Map apontariam para o conjunto certo de tarefas do Amazon ECS. Então, as APIs HTTP do API Gateway podem ser usadas para definir rotas de API e apontá-las para os serviços correspondentes do AWS Cloud Map.

Pergunta 38

Uma empresa de comércio eletrônico copiou 1 petabyte de dados de seu data center local para um bucket do Amazon S3 na **us-west-1** região usando um link do AWS Direct Connect. A empresa agora deseja configurar uma cópia única dos dados para outro bucket do Amazon S3 na **us-east-1** região. O data center local não permite o uso do AWS Snowball.

Como Arquiteto de Soluções, qual das seguintes opções pode ser usada para atingir esse objetivo? (Selecione duas)

R: Copie os dados do bucket de origem para o bucket de destino usando o comando `aws S3 sync`

R: Configure a replicação em lote do Amazon S3 para copiar objetos entre buckets do Amazon S3 em outra região usando o console do S3 e, em seguida, exclua a configuração de replicação

Opções corretas:

Copie os dados do bucket de origem para o bucket de destino usando o comando `aws S3 sync`

O comando `aws S3 sync` usa as APIs CopyObject para copiar objetos entre buckets do Amazon S3. O comando `sync` lista os buckets de origem e de destino para identificar objetos que estão no bucket de origem, mas que não estão no bucket de destino. O comando também identifica objetos no bucket de origem que têm datas de LastModified diferentes dos objetos que estão no bucket de destino. O comando `sync` em um bucket versionado copia apenas a versão atual do objeto – versões anteriores não são copiadas. Por padrão, isso preserva os metadados do objeto, mas as listas de controle de acesso (ACLs) são definidas como FULL_CONTROL para sua conta da AWS, o que remove quaisquer ACLs adicionais. Se a operação falhar, você poderá executar o comando `sync` novamente sem duplicar os objetos copiados anteriormente.

Você pode usar o comando assim:

```
aws s3 sync s3://DOC-EXAMPLE-BUCKET-SOURCE s3://DOC-EXAMPLE-BUCKET-TARGET
```


Configure a replicação em lote do Amazon S3 para copiar objetos entre buckets do Amazon S3 em outra região usando o console do S3 e, em seguida, exclua a configuração de replicação

O Amazon S3 Batch Replication fornece uma maneira de replicar objetos que existiam antes de uma configuração de replicação estar em vigor, objetos que foram replicados anteriormente e objetos que falharam na replicação. Isso é feito por meio do uso de um trabalho Batch Operations.

Observe que a replicação em lote é diferente da replicação em tempo real, que replica novos objetos de forma contínua e automática nos buckets do Amazon S3. Não é possível usar o console do AWS S3 diretamente para configurar a replicação entre regiões para objetos existentes. Por padrão, a replicação só oferece suporte à cópia de novos objetos do Amazon S3 após ser habilitada no console do AWS S3. A replicação permite a cópia automática e assíncrona de objetos entre buckets do Amazon S3. Os buckets configurados para replicação de objetos podem pertencer à mesma conta da AWS ou a contas diferentes. O objeto pode ser replicado para um único bucket de destino ou para vários buckets de destino. Os buckets de destino podem estar em diferentes regiões da AWS ou na mesma região do bucket de origem. Após concluir a configuração, você pode excluir a configuração de replicação, pois ela garante que a replicação em lote seja usada apenas para essa operação única de cópia de dados.

Se você quiser habilitar a replicação ao vivo para objetos existentes para seu bucket, entre em contato com o AWS Support e abra um ticket de suporte. Isso é necessário para garantir que a replicação esteja configurada corretamente.

Pergunta 39

Uma empresa de varejo está usando conexões VPN Site-to-Site da AWS para conectividade segura com seus recursos de nuvem da AWS a partir de seu data center local. Devido a um aumento no tráfego nas conexões VPN para a nuvem da AWS, os usuários estão enfrentando conectividade VPN mais lenta.

Qual das seguintes opções maximizará o rendimento da VPN?

R: Crie um AWS Transit Gateway com roteamento multicaminho de custo igual e adicione túneis VPN adicionais

Opção correta:

Crie um AWS Transit Gateway com roteamento multicaminho de custo igual e adicione túneis VPN adicionais

A conexão VPN é uma conexão segura entre seu equipamento local e seus VPCs. Cada conexão VPN tem dois túneis VPN que você pode usar para alta disponibilidade. Um túnel VPN é um link criptografado onde os dados podem passar da rede do cliente para ou da AWS. O diagrama a seguir mostra a conectividade de alto nível com gateways privados virtuais.

Com o AWS Transit Gateway, você pode simplificar a conectividade entre várias VPCs e também se conectar a qualquer VPC conectada ao AWS Transit Gateway com uma única conexão VPN. O AWS Transit Gateway também permite dimensionar a taxa de transferência de VPN IPsec com suporte a roteamento multicaminhos de custo igual (ECMP) em vários túneis VPN. Um único túnel VPN ainda tem uma taxa de transferência máxima de 1,25 Gbps. Se você estabelecer vários túneis VPN para um gateway de trânsito habilitado para ECMP, ele poderá ser dimensionado além do limite máximo padrão de 1,25 Gbps. Você também deve habilitar a opção de roteamento dinâmico no seu gateway de trânsito para poder aproveitar o ECMP para escalabilidade.

Pergunta 40

Uma empresa líder em comércio eletrônico executa sua infraestrutura de TI na AWS Cloud. A empresa tem um trabalho em lote em execução às 7h diariamente em um banco de dados Amazon RDS. Ela processa pedidos de remessa do dia anterior e geralmente obtém cerca de 2.000 registros que precisam ser processados sequencialmente em um trabalho em lote por meio de um script de shell. O processamento de cada registro leva cerca de 3 segundos.

Qual plataforma você recomenda para executar esse trabalho em lote?

R: Nuvem de computação elástica da Amazon (Amazon EC2)

Opção correta:

Nuvem de computação elástica da Amazon (Amazon EC2)

O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço web que fornece capacidade computacional segura e redimensionável na nuvem. Ele foi projetado para facilitar a computação em nuvem em escala web para desenvolvedores. A interface simples do serviço web do Amazon EC2 permite que você obtenha e configure capacidade com o mínimo de atrito. Ele oferece controle total sobre seus recursos de computação e permite que você execute no ambiente de computação comprovado da Amazon. O AWS Batch pode ser usado para planejar, agendar e executar suas cargas de trabalho de computação em lote em instâncias do Amazon EC2. O Amazon EC2 é a escolha certa, pois pode acomodar processamento em lote e executar scripts personalizados, conforme necessário.

Pergunta 41

A equipe de engenharia de uma empresa está executando cargas de trabalho em lote na Nuvem AWS. A equipe incorporou strings de conexão do banco de dados Amazon RDS em cada servidor web que hospeda o aplicativo principal. Após a falha em uma auditoria de segurança, a equipe está buscando uma abordagem diferente para armazenar os segredos do banco de dados com segurança e rotacionar automaticamente as credenciais do banco de dados.

Qual das seguintes soluções você recomendaria para atender a esse requisito?

R: Gerenciador de segredos da AWS

Opção correta:

Gerenciador de segredos da AWS

O AWS Secrets Manager permite que você rotacione, gerencie e recupere facilmente credenciais de banco de dados, chaves de API e outros segredos ao longo de seu ciclo de vida. Usuários e aplicativos recuperam segredos com uma chamada às APIs do Secrets Manager, eliminando a necessidade de codificar informações confidenciais em texto simples. O Secrets Manager oferece rotação de segredos com integração com Amazon RDS, Amazon Redshift e Amazon DocumentDB.

Pergunta 42

Uma empresa observou que seu Volume Elástico do Amazon EBS (io1) representa 90% do custo e os 10% restantes podem ser atribuídos à instância do Amazon EC2. As métricas do Amazon CloudWatch relatam que tanto a instância do Amazon EC2 quanto o volume do Amazon EBS estão subutilizados. As métricas do Amazon CloudWatch também mostram que o volume do Amazon EBS apresenta picos ocasionais de E/S. Toda a infraestrutura é gerenciada pelo AWS CloudFormation.

Como arquiteto de soluções, o que você propõe para reduzir os custos?

R: Converter o volume EBS da instância do Amazon EC2 para gp2

Opção correta:

O Amazon EBS oferece vários tipos de volume, que diferem em características de desempenho e preço, para que você possa adaptar o desempenho e o custo do seu armazenamento às necessidades dos seus aplicativos. Os tipos de volume se dividem em duas categorias:

Volumes suportados por SSD otimizados para cargas de trabalho transacionais envolvendo operações frequentes de leitura/gravação com tamanho pequeno de E/S, onde o atributo de desempenho dominante é IOPS.

Volumes suportados por HDD otimizados para grandes cargas de trabalho de streaming onde a taxa de transferência (medida em MiB/s) é uma medida de desempenho melhor do que IOPS

Os volumes SSD com IOPS provisionados (io1) são projetados para atender às necessidades de cargas de trabalho com uso intensivo de E/S, especialmente cargas de trabalho de banco de dados, que são sensíveis ao desempenho e à consistência do armazenamento. Ao contrário do gp2, que usa um modelo de bucket e crédito para calcular o desempenho, um volume io1 permite que você especifique uma taxa de IOPS consistente ao criá-lo, e o Amazon EBS fornece o desempenho provisionado em 99,9% das vezes.

Converter o volume EBS da instância do Amazon EC2 para gp2

Os volumes SSD de uso geral (gp2) oferecem armazenamento econômico, ideal para uma ampla gama de cargas de trabalho. Esses volumes oferecem latências de milissegundos de um dígito e a capacidade de atingir picos de até 3.000 IOPS por um período prolongado. Entre um mínimo de 100 IOPS (a 33,33 GiB e menos) e um máximo de 16.000 IOPS (a 5.334 GiB e mais), o desempenho básico é escalável linearmente a 3 IOPS por GiB de tamanho do volume. A AWS projeta volumes gp2 para oferecer um desempenho provisionado de 99% de tempo de atividade. Um volume gp2 pode variar de 1 GiB a 16 TiB. Portanto, o gp2 é a escolha certa, pois é mais econômico que o io1 e também permite um aumento no desempenho quando necessário.

Pergunta 43

O que este snippet do AWS CloudFormation faz? (Selecione três)

```
SecurityGroupIngress:
  - IpProtocol: tcp
    FromPort: 80
    ToPort: 80
    CidrIp: 0.0.0.0/0
  - IpProtocol: tcp
    FromPort: 22
    ToPort: 22
    CidrIp: 192.168.1.1/32
```

Seleção correta

R: Ele permite que o tráfego flua de um IP na porta 22

R: Ele configura as regras de entrada de um grupo de segurança

R: Permite que qualquer IP passe pela porta HTTP

Opções corretas:

Permite que qualquer IP passe pela porta HTTP

Ele configura as regras de entrada de um grupo de segurança

Ele permite que o tráfego flua de um IP na porta 22

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, usaremos 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. Quando decidimos se permitimos ou não o tráfego para uma instância, avaliamos todas as regras de todos os grupos de segurança associados a ela.

As seguintes são as características das regras de grupo de segurança: 1. Por padrão, os grupos de segurança permitem todo o tráfego de saída. 2. As regras de grupo de segurança são sempre permissivas; você não pode criar regras que neguem acesso. 3. Os grupos de segurança são com estado O AWS CloudFormation fornece uma linguagem comum para você modelar e provisionar recursos de aplicativos da AWS e de terceiros em seu ambiente de nuvem. O AWS CloudFormation permite que você use linguagens de programação ou um arquivo de texto simples para modelar e provisionar, de forma automatizada e segura, todos os recursos necessários para seus aplicativos em todas as regiões e contas. Isso lhe dá uma única fonte de verdade para seus recursos da AWS e de terceiros.

Considerando o snippet do AWS CloudFormation fornecido, `0.0.0.0/0` significa qualquer IP, não o IP `0.0.0.0`. Entrada significa tráfego que entra na sua instância, e Grupos de Segurança são diferentes de NACL. Cada "-" em nossa regra de grupo de segurança representa uma regra diferente (sintaxe YAML).

Portanto, o snippet do AWS CloudFormation cria duas regras de entrada do Grupo de Segurança que permitem que qualquer IP passe pela porta HTTP e permite que o tráfego flua de um IP de origem (192.168.1.1) na porta 22.

Pergunta 44

Você está trabalhando para uma empresa de software como serviço (SaaS) como arquiteto de soluções e ajuda a projetar soluções para os clientes da empresa. Um dos clientes é um banco e tem um requisito para colocar um IP público na lista de permissões quando o banco está acessando serviços externos pela internet.

Qual escolha arquitetônica você recomenda para manter alta disponibilidade, suportar escalonamento para até 10 instâncias e atender aos requisitos do banco?

R: Use um balanceador de carga de rede com um grupo de dimensionamento automático

Opção correta:

Use um balanceador de carga de rede com um grupo de dimensionamento automático

O Network Load Balancer é mais adequado para casos de uso que envolvem cargas de trabalho de baixa latência e alto throughput, com escalabilidade para milhões de solicitações por segundo. O Network Load Balancer opera no nível de conexão (Camada 4), roteando conexões para destinos – instâncias do Amazon EC2, microsserviços e contêineres – dentro da Amazon Virtual Private Cloud (Amazon VPC) com base em dados de protocolo IP. Um Network Load Balancer funciona na quarta camada do modelo Open Systems Interconnection (OSI). Ele pode lidar com milhões de solicitações por segundo.

Os balanceadores de carga de rede expõem um IP fixo à web pública, permitindo que seu aplicativo seja alcançado previsivelmente usando esse IP, ao mesmo tempo em que permite que você dimensione seu aplicativo por trás do balanceador de carga de rede usando um ASG.

Pergunta 45

Um aplicativo web CRM foi escrito como um monólito em PHP e está enfrentando problemas de escalabilidade devido a gargalos de desempenho. O CTO quer reprojeter para arquitetura de microsserviços e expor seu aplicativo do mesmo balanceador de carga, vinculado a diferentes grupos-alvo com diferentes URLs: checkout.mycorp.com, www.mycorp.com, yourcorp.com/profile e yourcorp.com/search. O CTO gostaria de expor todos esses URLs como endpoints HTTPS para fins de segurança.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como uma solução que requer esforço MÍNIMO de configuração?

R: Use o certificado Secure Sockets Layer (certificado SSL) com SNI

Opção correta:

Use o certificado Secure Sockets Layer (certificado SSL) com SNI

Você pode hospedar vários aplicativos protegidos por TLS, cada um com seu próprio certificado TLS, em um único balanceador de carga. Para usar o SNI, basta vincular vários certificados ao mesmo ouvinte seguro no seu balanceador de carga. O ALB escolherá automaticamente o certificado TLS ideal para cada cliente.

A seleção de certificados inteligentes do ALB vai além do SNI. Além de conter uma lista de nomes de domínio válidos, os certificados também descrevem o tipo de troca de chaves e criptografia suportados pelo servidor, bem como o algoritmo de assinatura (SHA2, SHA1, MD5) usado para assinar o certificado.

Com o suporte a SNI, a AWS facilita o uso de mais de um certificado com o mesmo ALB. O motivo mais comum para usar vários certificados é lidar com diferentes domínios com o mesmo balanceador de carga. Sempre foi possível usar certificados curinga e SAN (Subject-Alternate-Name) com ALB, mas eles apresentam limitações. Certificados curinga funcionam apenas para subdomínios relacionados que correspondem a um padrão simples e, embora os certificados SAN possam suportar muitos domínios diferentes, a mesma autoridade certificadora precisa autenticar cada um deles. Isso significa que

you need to authenticate and reprovision your certificate whenever you add a new domain.

Pergunta 46

A social media application of niche allows users to connect with athletes. As an architect of solutions, you designed the architecture of the application to be totally serverless, using the Amazon API Gateway and the AWS Lambda. The backend uses a table of the Amazon DynamoDB. Some of the famous athletes who use the application are very popular and, for this reason, the Amazon DynamoDB increased the units of capacity of reading (RCUs). Even so, the application is presenting a problem of active partition.

What can you do to improve the performance of the Amazon DynamoDB and eliminate the problem of active partition without much refactoring of applications?

R: Use o Amazon DynamoDB DAX

Opção correta:

Use o Amazon DynamoDB DAX

The Amazon DynamoDB is a database of key-value and documents that offers performance of milliseconds in any scale. It is a database totally managed, multi-regional, multi-tenant and durable, with integrated security, backup and restoration and cache in memory for applications in internet scale.

The Amazon DynamoDB Accelerator (DAX) is a cache in memory totally managed and highly available for the DynamoDB that offers a performance improvement of up to 10x - from milliseconds to microseconds - even with millions of requests per second. The DAX does all the heavy work necessary to add acceleration in memory to its tables of the DynamoDB, without requiring that the developers manage the invalidation of the cache, the filling of data or the management of the cluster.

The DAX will be transparent, it will not require refactoring of the application and will store in cache the "shortcut keys". Therefore, this is the correct option.

Pergunta 47

A company of CRM has an application of software as a service (SaaS) that feeds updates for other internal and external applications. The SaaS application and the internal applications are being migrated to use AWS services for this communication between applications.

As an architect of solutions, which of the options to follow you would suggest to decouple the architecture in an asynchronous way?

Resposta correta

R: Use o Amazon EventBridge para desacoplar a arquitetura do sistema

Opção correta:

Use o Amazon EventBridge para desacoplar a arquitetura do sistema

Both the Amazon EventBridge and the Amazon SNS can be used to develop event-driven applications, but for this use case, the EventBridge is the correct option.

The Amazon EventBridge is recommended when you want to create an application that reacts to events of SaaS applications and/or AWS services. The Amazon EventBridge is the only service based on events that integrates directly with SaaS partners of third parties. The Amazon EventBridge also ingests automatically events of more than 90 AWS services without requiring that the developers create resources in their accounts. In addition, the Amazon EventBridge uses a predefined structure based on JSON for events and allows you to create rules that are applied to the entire event body to select events to be routed to a destination. The Amazon EventBridge currently offers support for more than 15 AWS services as destinations, including AWS Lambda, Amazon SQS, Amazon SNS and Amazon Kinesis Streams and Firehose, among others. At launch, the Amazon EventBridge has a limited transfer rate (consult the service limits), which can be increased by request, and a typical latency of about half a second.

Pergunta 48

Uma empresa de saúde está avaliando opções de armazenamento no Amazon S3 para atender às diretrizes regulatórias. Os dados devem ser armazenados no Amazon S3 de forma que não possam ser excluídos até que o prazo regulatório expire.

Como arquiteto de soluções, qual das opções a seguir você recomendaria para o requisito fornecido?
R: Usar bloqueio de objeto do Amazon S3

Opção correta:

Usar bloqueio de objeto do Amazon S3

O Bloqueio de Objetos do Amazon S3 é um recurso do Amazon S3 que permite armazenar objetos usando um modelo WORM (gravação única, leitura múltipla). Você pode usar a proteção WORM em cenários em que é fundamental que os dados não sejam alterados ou excluídos após a gravação. Se sua empresa precisa atender às normas de conformidade no setor financeiro ou de saúde, ou se você simplesmente deseja capturar uma cópia valiosa dos registros comerciais para auditoria e reconciliação posteriores, o Bloqueio de Objetos do Amazon S3 é a ferramenta ideal para você. O Bloqueio de Objetos pode ajudar a impedir que objetos sejam excluídos ou substituídos por um período fixo ou indefinidamente.

Pergunta 49

A equipe de desenvolvimento de uma empresa de mídia social quer lidar com algumas consultas complicadas, como "Qual é o número de curtidas nos vídeos postados pelos amigos do usuário A?".

Como arquiteto de soluções, qual dos seguintes serviços de banco de dados da AWS você sugeriria como o MELHOR para lidar com esses casos de uso?

R: Amazon Netuno

Opção correta:

Amazon Netuno

O Amazon Neptune é um serviço de banco de dados de gráficos rápido, confiável e totalmente gerenciado que facilita a criação e a execução de aplicativos que funcionam com conjuntos de dados altamente conectados. O núcleo do Amazon Neptune é um mecanismo de banco de dados de gráficos de alto desempenho e desenvolvido especificamente para armazenar bilhões de relacionamentos e consultar o gráfico com latência de milissegundos. O Neptune potencializa casos de uso de gráficos, como mecanismos de recomendação, detecção de fraudes, gráficos de conhecimento, descoberta de medicamentos e segurança de rede.

O Amazon Neptune é altamente disponível, com réplicas de leitura, recuperação de ponto no tempo, backup contínuo para o Amazon S3 e replicação em Zonas de Disponibilidade. O Neptune é seguro com suporte para conexões de cliente criptografadas HTTPS e criptografia em repouso. O Neptune é totalmente gerenciado, então você não precisa mais se preocupar com tarefas de gerenciamento de banco de dados, como provisionamento de hardware, aplicação de patches de software, instalação, configuração ou backups.

O Amazon Neptune pode processar de forma rápida e fácil grandes conjuntos de perfis de usuários e interações para criar aplicativos de redes sociais. O Neptune permite consultas gráficas altamente interativas com alto rendimento para trazer recursos sociais para seus aplicativos. Por exemplo, se você estiver criando um feed social em seu aplicativo, poderá usar o Neptune para fornecer resultados que priorizem mostrar aos seus usuários as últimas atualizações de suas famílias, de amigos cujas atualizações eles 'curtem' e de amigos que moram perto deles.

Pergunta 50

Um desenvolvedor júnior baixou um exemplo de política de bucket do Amazon S3 para fazer alterações com base nas novas políticas de acesso de toda a empresa. Ele solicitou sua ajuda para entender essa política de bucket.

Como arquiteto de soluções, qual das seguintes opções você identificaria como a descrição correta para a política em questão?

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

R: Ele autoriza um roteamento interdomínio sem classes (CIDR) inteiro, exceto um endereço IP para acessar o bucket do Amazon S3

Opção correta:

Ele autoriza um roteamento interdomínio sem classes (CIDR) inteiro, exceto um endereço IP para acessar o bucket do Amazon S3

Você gerencia o acesso na AWS criando políticas e anexando-as a identidades do IAM (usuários, grupos de usuários ou funções) ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando um principal do IAM (usuário ou função) faz uma solicitação. As permissões nas políticas determinam se a solicitação é permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. A AWS oferece suporte a seis tipos de políticas: políticas baseadas em identidade, políticas baseadas em recursos, limites de permissões, SCPs do AWS Organizations, ACLs e políticas de sessão. Vamos analisar a política de bucket um passo de cada vez:

O snippet `"Effect": "Allow"` implica um efeito de permissão. O snippet `"Principal": "*"` implica qualquer Principal. O snippet `"Action": "s3:*"` implica qualquer API do Amazon S3. O snippet `"Resource": "arn:aws:s3:::examplebucket/*"` implica que o recurso pode ser o bucket `examplebucket` e seu conteúdo. Considere o último snippet da política de bucket fornecida: `"Condition": { "IpAddress": {"aws:SourceIp": "54.240.143.0/24"}, "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"} }` Este snippet implica que, se o IP de origem estiver no bloco CIDR "54.240.143.0/24" (== 54.240.143.0 - 54.240.143.255), ele terá permissão para acessar o bucket `examplebucket` e seu conteúdo. No entanto, o IP de origem não pode estar no CIDR "54.240.143.188/32" (== 1 IP, 54.240.143.188/32), o que significa que um endereço IP está explicitamente bloqueado para acessar o bucket `examplebucket` e seu conteúdo.

Exemplo de políticas de Bucket:

Pergunta 51

Um Elastic Load Balancer marcou todas as instâncias do Amazon EC2 no grupo de destino como não íntegras. Surpreendentemente, quando um desenvolvedor insere o endereço IP das instâncias do Amazon EC2 no navegador, ele consegue acessar o site. Qual poderia ser o motivo pelo qual as instâncias estão sendo marcadas como não íntegras? (Selecione duas)

R: A rota para a verificação de integridade está mal configurada

R: O grupo de segurança da instância do Amazon EC2 não permite tráfego do grupo de segurança do Application Load Balancer

Opções corretas:

O grupo de segurança da instância do Amazon EC2 não permite tráfego do grupo de segurança do Application Load Balancer

A rota para a verificação de integridade está mal configurada

- Um Application Load Balancer envia periodicamente solicitações aos seus alvos registrados para testar seu status. Esses testes são chamados de verificações de integridade.

Cada nó do balanceador de carga encaminha solicitações apenas para os destinos íntegros nas Zonas de Disponibilidade (AZs) habilitadas para o balanceador de carga. Cada nó do balanceador de carga verifica a integridade de cada destino, usando as configurações de verificação de integridade dos grupos de destinos nos quais o destino está registrado. Se um grupo de destinos contiver apenas destinos registrados com problemas de integridade, os nós do balanceador de carga encaminharão as solicitações entre seus destinos com problemas de integridade.

Você deve garantir que seu balanceador de carga possa se comunicar com destinos registrados tanto na porta do listener quanto na porta de verificação de integridade. Sempre que adicionar um listener ao seu balanceador de carga ou atualizar a porta de verificação de integridade para um grupo de destino usado pelo balanceador de carga para rotear solicitações, você deve verificar se os grupos de segurança associados ao balanceador de carga permitem tráfego na nova porta em ambas as direções.

Pergunta 52

Uma empresa de mídia social deseja ter a capacidade de alterar dinamicamente o tamanho de uma área geográfica da qual o tráfego é roteado para um recurso de servidor específico.

Qual recurso do Amazon Route 53 pode ajudar a atingir essa funcionalidade?

R: Roteamento de geoproximidade

Opção correta:

Roteamento de geoproximidade

O roteamento por geoproximidade permite que o Amazon Route 53 direcione o tráfego para seus recursos com base na localização geográfica dos seus usuários e dos seus recursos. Você também pode optar por direcionar mais ou menos tráfego para um determinado recurso especificando um valor, conhecido como desvio. Um desvio expande ou reduz o tamanho da região geográfica da qual o tráfego é roteado para um recurso.

Para alterar opcionalmente o tamanho da região geográfica da qual o Amazon Route 53 roteia o tráfego para um recurso, especifique o valor aplicável para o desvio: 1. Para expandir o tamanho da região geográfica da qual o Amazon Route 53 roteia o tráfego para um recurso, especifique um número inteiro positivo de 1 a 99 para o desvio. O Amazon Route 53 reduz o tamanho das regiões adjacentes.

1. Para reduzir o tamanho da região geográfica da qual o Amazon Route 53 roteia o tráfego para um recurso, especifique um desvio negativo de -1 a -99. O Amazon Route 53 expande o tamanho das regiões adjacentes.

Pergunta 53

Uma equipe de desenvolvimento configurou o Elastic Load Balancing para roteamento baseado em host. A ideia é dar suporte a vários subdomínios e diferentes domínios de nível superior.

A regra *.example.com corresponde a qual das seguintes opções?

R: teste.exemplo.com

Opção correta:

teste.exemplo.com

Você pode usar condições de host para definir regras que roteiam solicitações com base no nome do host no cabeçalho do host (também conhecido como roteamento baseado em host). Isso permite que você suporte vários subdomínios e diferentes domínios de nível superior usando um único balanceador de carga.

Um nome de host não diferencia maiúsculas de minúsculas, pode ter até 128 caracteres e pode conter qualquer um dos seguintes caracteres: 1. A-Z, a-z, 0-9 2. - 3. * (corresponde a 0 ou mais caracteres) 4. ? (corresponde exatamente a 1 caractere)

Você deve incluir pelo menos um caractere "." Você pode incluir apenas caracteres alfabéticos após o caractere "." final.

A regra *.example.com corresponde a test.example.com, mas não corresponde a example.com.

Pergunta 54

Uma empresa desenvolveu um site popular de compartilhamento de fotos usando um padrão sem servidor na Nuvem AWS usando o Amazon API Gateway e o AWS Lambda. O backend usa um banco de dados Amazon RDS PostgreSQL. O site está com alto tráfego de leitura e as funções do AWS Lambda estão colocando uma carga de leitura maior no banco de dados Amazon RDS. A equipe de arquitetura está planejando aumentar a taxa de transferência de leitura do banco de dados sem alterar a lógica central do aplicativo. Como Arquiteto de Soluções, o que você recomenda?

R: Usar réplicas de leitura do Amazon RDS

Opção correta:

Usar réplicas de leitura do Amazon RDS

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

Pergunta 55

A equipe de engenharia de uma empresa de e-commerce foi encarregada de migrar para uma arquitetura sem servidor. A equipe quer se concentrar nos principais pontos a serem considerados ao usar o AWS Lambda como base para essa arquitetura.

Como Arquiteto de Soluções, qual das seguintes opções você identificaria como correta para o requisito fornecido? (Selecione três)

R: Como as funções do AWS Lambda podem ser dimensionadas extremamente rápido, é uma boa ideia implantar um alarme do Amazon CloudWatch que notifique sua equipe quando as métricas de função, como `ConcurrentExecutions` ou `Invocations exceeds the expected threshold`

R: Se você pretende reutilizar o código em mais de uma função do AWS Lambda, considere criar uma camada do AWS Lambda para o código reutilizável

R: Por padrão, as funções do AWS Lambda sempre operam a partir de uma VPC de propriedade da AWS e, portanto, têm acesso a qualquer endereço público de internet ou APIs públicas da AWS. Uma vez habilitada para VPC, uma função do AWS Lambda precisará de uma rota por meio de um gateway de Tradução de Endereços de Rede (gateway NAT) em uma sub-rede pública para acessar recursos públicos.

Opções corretas:

Por padrão, as funções do AWS Lambda sempre operam a partir de uma VPC de propriedade da AWS e, portanto, têm acesso a qualquer endereço público de internet ou APIs públicas da AWS. Uma vez habilitada para VPC, uma função do AWS Lambda precisará de uma rota por meio de um gateway de Tradução de Endereços de Rede (gateway NAT) em uma sub-rede pública para acessar recursos públicos. As funções do AWS Lambda sempre operam a partir de uma VPC de propriedade da AWS. Por padrão, sua função tem capacidade total para fazer solicitações de rede para qualquer endereço público de internet – isso inclui acesso a qualquer uma das APIs públicas da AWS. Por exemplo, sua função pode interagir com APIs do AWS DynamoDB para **PutItem** consultar registros. Você só deve habilitar suas funções para acesso à VPC quando precisar interagir com um recurso privado localizado em uma sub-rede privada. Uma instância do Amazon RDS é um bom exemplo.

Depois que sua função estiver habilitada para VPC, todo o tráfego de rede da sua função estará sujeito às regras de roteamento da sua VPC/Subnet. Se sua função precisar interagir com um recurso público, você precisará de uma rota por meio de um gateway NAT em uma subnet pública.

Como as funções do AWS Lambda podem ser dimensionadas extremamente rápido, é uma boa ideia implantar um alarme do Amazon CloudWatch que notifique sua equipe quando as métricas de função, como **ConcurrentExecutions ou **Invocations exceeds the expected threshold****

- Como as funções do AWS Lambda podem ser dimensionadas extremamente rápido, isso significa que você deve ter controles em vigor para notificá-lo quando houver um pico de simultaneidade. Uma boa ideia é implantar um Amazon CloudWatch Alarm que notifique sua equipe quando métricas de função como **ConcurrentExecutions** ou **Invocations exceeds your threshold** . Você deve criar um AWS Budget para poder monitorar os custos diariamente.

Se você pretende reutilizar o código em mais de uma função do AWS Lambda, considere criar uma camada do AWS Lambda para o código reutilizável

Você pode configurar sua função do AWS Lambda para extrair código e conteúdo adicionais na forma de camadas. Uma camada é um arquivo ZIP que contém bibliotecas, um tempo de execução personalizado ou outras dependências. Com camadas, você pode usar bibliotecas em sua função sem precisar incluí-las em seu pacote de implantação. As camadas permitem que você mantenha seu pacote de implantação pequeno, o que facilita o desenvolvimento. Uma função pode usar até 5 camadas por vez.

Você pode criar camadas ou usar camadas publicadas pela AWS e por outros clientes da AWS. As camadas oferecem suporte a políticas baseadas em recursos para conceder permissões de uso de camadas a contas específicas da AWS, organizações da AWS ou a todas as contas. O tamanho total descompactado da função e de todas as camadas não pode exceder o limite de tamanho do pacote de implantação descompactado de 250 megabytes.

Pergunta 56

Uma empresa de análise de Big Data grava dados e arquivos de log em buckets do Amazon S3. A empresa agora quer transmitir os arquivos de dados existentes, bem como quaisquer atualizações de arquivo em andamento do Amazon S3 para o Amazon Kinesis Data Streams.

Como arquiteto de soluções, qual das opções a seguir você sugeriria como a maneira mais rápida possível de criar uma solução para esse requisito?

R: Aproveite o AWS Database Migration Service (AWS DMS) como uma ponte entre o Amazon S3 e o Amazon Kinesis Data Streams

Opção correta:

Aproveite o AWS Database Migration Service (AWS DMS) como uma ponte entre o Amazon S3 e o Amazon Kinesis Data Streams

Você pode fazer isso usando o AWS Database Migration Service (AWS DMS). O AWS DMS permite que você migre dados facilmente de fontes suportadas para bancos de dados relacionais, data warehouses, plataformas de streaming e outros armazenamentos de dados na nuvem da AWS.

O requisito fornecido precisa que a funcionalidade seja implementada no menor tempo possível. Você pode usar o AWS DMS para tais requisitos de processamento de dados. O AWS DMS permite que você expanda o aplicativo existente para transmitir dados do Amazon S3 para o Amazon Kinesis Data Streams para análises em tempo real sem escrever e manter um novo código. O AWS DMS oferece suporte à especificação do Amazon S3 como a origem e serviços de streaming como Kinesis e Amazon Managed Streaming of Kafka (Amazon MSK) como o destino. O AWS DMS permite a migração de arquivos de captura de dados completos e alterados (CDC) para esses serviços. O AWS DMS executa essa tarefa imediatamente, sem nenhuma configuração complexa ou desenvolvimento de código. Você também pode configurar uma instância de replicação do AWS DMS para aumentar ou diminuir dependendo da carga de trabalho.

O AWS DMS oferece suporte ao Amazon S3 como origem e ao Kinesis como destino, portanto, os dados armazenados em um bucket do S3 são transmitidos para o Kinesis. Vários consumidores, como AWS Lambda, Amazon Kinesis Data Firehose, Amazon Kinesis Data Analytics e Kinesis Consumer Library (KCL), podem consumir os dados simultaneamente para executar análises em tempo real no conjunto de dados. Cada serviço da AWS nessa arquitetura pode ser dimensionado de forma independente, conforme necessário.

Arquitetura da solução proposta:

Pergunta 57

Uma empresa de processamento de Big Data criou uma estrutura de processamento de dados distribuídos que apresenta melhor desempenho se o desempenho da rede entre as máquinas de processamento for alto. O aplicativo precisa ser implantado na AWS, e a empresa considera apenas o desempenho como principal parâmetro.

Como arquiteto de soluções, qual implantação você recomenda?

Use um grupo de posicionamento de cluster

Opção correta:

Ao iniciar uma nova instância do Amazon EC2, o serviço EC2 tenta posicionar a instância de forma que todas as suas instâncias sejam distribuídas pelo hardware subjacente para minimizar falhas correlacionadas. Você pode usar grupos de posicionamento para influenciar o posicionamento de um grupo de instâncias interdependentes para atender às necessidades da sua carga de trabalho. Dependendo do tipo de carga de trabalho, você pode criar um grupo de posicionamento usando uma das seguintes estratégias de posicionamento:

Cluster – agrupa instâncias próximas umas das outras dentro de uma Zona de Disponibilidade (AZ). Essa estratégia permite que as cargas de trabalho atinjam o desempenho de rede de baixa latência necessário para comunicação nó a nó fortemente acoplada, típica de aplicativos HPC.

Partição – espalha suas instâncias em partições lógicas de modo que grupos de instâncias em uma partição não compartilhem o hardware subjacente com grupos de instâncias em partições diferentes. Essa estratégia é normalmente usada por grandes cargas de trabalho distribuídas e replicadas, como Hadoop, Cassandra e Kafka.

Espalhar – coloca estritamente um pequeno grupo de instâncias em hardware subjacente distinto para reduzir falhas correlacionadas.

Não há custos para criar um grupo de colocação.

Use um grupo de posicionamento de cluster

Um grupo de posicionamento de cluster é um agrupamento lógico de instâncias dentro de uma única Zona de Disponibilidade (AZ). Um grupo de posicionamento de cluster pode abranger VPCs pareadas na mesma Região. Instâncias no mesmo grupo de posicionamento de cluster desfrutam de um limite de taxa

de transferência por fluxo maior, de até 10 Gbps para tráfego TCP/IP, e são colocadas no mesmo segmento de largura de banda de alta bissecção da rede.

Os grupos de posicionamento de cluster são recomendados para aplicativos que se beneficiam de baixa latência de rede, alta taxa de transferência de rede ou ambos. Eles também são recomendados quando a maioria do tráfego de rede está entre as instâncias no grupo. Para fornecer a menor latência e o maior desempenho de rede de pacotes por segundo para seu grupo de posicionamento, escolha um tipo de instância que suporte rede aprimorada.

Pergunta 58

Uma empresa de TI executa uma carga de trabalho de computação de alto desempenho (HPC) na AWS. A carga de trabalho exige alta taxa de transferência de rede e desempenho de rede de baixa latência, além de comunicações nó a nó fortemente acopladas. As instâncias do Amazon EC2 são dimensionadas corretamente para capacidade de computação e armazenamento e são iniciadas usando opções padrão.

Qual das seguintes soluções pode ser usada para melhorar o desempenho da carga de trabalho?

R: Selecione um grupo de posicionamento de cluster ao iniciar instâncias do Amazon EC2

Opção correta:

Selecione um grupo de posicionamento de cluster ao iniciar instâncias do Amazon EC2

Ao iniciar uma nova instância do Amazon EC2, o serviço EC2 tenta posicionar a instância de forma que todas as suas instâncias sejam distribuídas pelo hardware subjacente para minimizar falhas correlacionadas. Você pode usar grupos de posicionamento para influenciar o posicionamento de um grupo de instâncias interdependentes para atender às necessidades da sua carga de trabalho.

O grupo de posicionamento de cluster agrupa instâncias próximas umas das outras dentro de uma Zona de Disponibilidade (AZ). Essa estratégia permite que as cargas de trabalho atinjam o desempenho de rede de baixa latência necessário para a comunicação nó a nó fortemente acoplada, típica de aplicações de HPC.

Pergunta 59

Você tem um bucket do Amazon S3 que contém arquivos em duas pastas diferentes - `s3://my-bucket/images` e `s3://my-bucket/thumbnails`. Quando uma imagem é carregada pela primeira vez e é nova, ela é visualizada várias vezes. Mas depois de 45 dias, a análise prova que os arquivos de imagem são, em média, raramente solicitados, mas as miniaturas ainda são. Depois de 180 dias, você gostaria de arquivar os arquivos de imagem e as miniaturas. No geral, você gostaria que a solução permanecesse altamente disponível para evitar que desastres acontecessem em uma Zona de Disponibilidade (AZ) inteira.

Como você pode implementar uma estratégia de custo eficiente para seu bucket Amazon S3? (Selecione duas)

R: Crie uma política de ciclo de vida para fazer a transição de objetos para o Amazon S3 Standard IA usando um prefixo após 45 dias

R: Crie uma política de ciclo de vida para fazer a transição de todos os objetos para o Amazon S3 Glacier após 180 dias

Opções corretas:

Para gerenciar seus objetos do S3 e armazená-los de forma econômica durante todo o seu ciclo de vida, configure o Ciclo de Vida do Amazon S3. Uma configuração do Ciclo de Vida do S3 é um conjunto de regras que definem as ações que o Amazon S3 aplica a um grupo de objetos. Existem dois tipos de ações:

Ações de transição – Defina quando os objetos são transferidos para outra classe de armazenamento. Por exemplo, você pode optar por transferir objetos para a classe de armazenamento S3 Standard-IA 30 dias após criá-los ou arquivá-los na classe de armazenamento S3 Glacier um ano após criá-los.

Ações de expiração – Defina quando os objetos expiram. O Amazon S3 exclui objetos expirados em seu

nome.

Crie uma política de ciclo de vida para fazer a transição de objetos para o Amazon S3 Standard IA usando um prefixo após 45 dias

O Amazon S3 Standard-IA é para dados que são acessados com menos frequência, mas exigem acesso rápido quando necessário. O Amazon S3 Standard-IA oferece alta durabilidade, alto rendimento e baixa latência do S3 Standard, com um baixo preço de armazenamento por gigabyte e taxa de recuperação por gigabyte. Essa combinação de baixo custo e alto desempenho torna o Amazon S3 Standard-IA ideal para armazenamento de longo prazo, backups e como um armazenamento de dados para arquivos de recuperação de desastres. A taxa mínima de duração do armazenamento é de 30 dias. Como o caso de uso menciona, após 45 dias, os arquivos de imagem raramente são solicitados, mas as miniaturas ainda são. Portanto, você precisa usar um prefixo ao configurar a Política de Ciclo de Vida para que apenas os objetos no bucket `s3://my-bucket/images` sejam transferidos para a IA Padrão e não todos os objetos no bucket.

Crie uma política de ciclo de vida para fazer a transição de todos os objetos para o Amazon S3 Glacier após 180 dias

O Amazon S3 Glacier e o S3 Glacier Deep Archive são classes de armazenamento em nuvem do Amazon S3 seguras, duráveis e de baixíssimo custo para arquivamento de dados e backup de longo prazo. Elas foram projetadas para oferecer durabilidade de 99,999999999% e oferecem recursos abrangentes de segurança e conformidade que podem ajudar a atender até mesmo aos requisitos regulatórios mais rigorosos.

Pergunta 60

Uma empresa decidiu mover suas cargas de trabalho secundárias, como backups e arquivos, para a nuvem AWS. O CTO deseja mover os dados armazenados em fitas físicas para a nuvem, sem alterar seus fluxos de trabalho atuais de backup de fita. A empresa mantém petabytes de dados em fitas e precisa de uma solução com custo otimizado para mover esses dados para a nuvem.

Qual é a solução ideal que atende a esses requisitos e ao mesmo tempo mantém os custos no mínimo?

R: Use o Tape Gateway, que pode ser usado para mover dados de fita no local para a AWS Cloud. Então, as classes de armazenamento de arquivamento do Amazon S3 podem ser usadas para armazenar dados de forma econômica por anos

Opção correta:

Use o Tape Gateway, que pode ser usado para mover dados de fita no local para a AWS Cloud. Então, as classes de armazenamento de arquivamento do Amazon S3 podem ser usadas para armazenar dados de forma econômica por anos

O Tape Gateway permite que você substitua o uso de fitas físicas no local por fitas virtuais na AWS sem alterar os fluxos de trabalho de backup existentes. O Tape Gateway oferece suporte a todos os principais aplicativos de backup e armazena em cache fitas virtuais no local para acesso de dados de baixa latência. O Tape Gateway criptografa dados entre o gateway e a AWS para transferência segura de dados e compacta dados durante a transição de fitas virtuais entre o Amazon S3 e o Amazon S3 Glacier, ou o Amazon S3 Glacier Deep Archive, para minimizar os custos de armazenamento.

O Tape Gateway compacta e armazena fitas virtuais arquivadas nas classes de armazenamento de menor custo do Amazon S3, Amazon S3 Glacier e Amazon S3 Glacier Deep Archive. Isso torna possível para você reter dados de longo prazo na Nuvem AWS a um custo muito baixo. Com o Tape Gateway, você paga apenas pelo que consome, sem compromissos mínimos e sem taxas iniciais.

O Tape Gateway armazena suas fitas virtuais em buckets S3 gerenciados pelo serviço AWS Storage Gateway, para que você não precise gerenciar seu próprio armazenamento Amazon S3. O Tape Gateway integra-se com todos os principais aplicativos de backup, permitindo que você comece a usar o armazenamento em nuvem para backup e arquivamento no local sem nenhuma alteração em seus fluxos de trabalho de backup e arquivamento.

Visão geral do Tape Gateway:

Pergunta 61

Uma empresa de compartilhamento de música utiliza um balanceador de carga de rede para direcionar o tráfego para 5 instâncias do Amazon EC2 gerenciadas por um grupo de Auto Scaling. Quando uma música muito popular é lançada, o grupo de Auto Scaling escala para 100 instâncias, e a empresa incorre em altas taxas de rede e computação.

A empresa quer uma solução para reduzir os custos sem alterar nenhum código do aplicativo. O que você recomenda?

R: Use uma distribuição do Amazon CloudFront

Opção correta:

Use uma distribuição do Amazon CloudFront

O Amazon CloudFront é um serviço rápido de rede de distribuição de conteúdo (CDN) que entrega com segurança dados, vídeos, aplicativos e APIs para clientes em todo o mundo, com baixa latência e altas velocidades de transferência, tudo em um ambiente amigável ao desenvolvedor.

Os pontos de presença (POPs) (localizações de borda) do Amazon CloudFront garantem que conteúdo popular seja disponibilizado rapidamente aos seus espectadores. O CloudFront também possui caches de borda regionais que aproximam mais do seu conteúdo dos seus espectadores, mesmo quando o conteúdo não é popular o suficiente para permanecer em um POP, ajudando a melhorar o desempenho desse conteúdo.

Os edge caches regionais ajudam com todos os tipos de conteúdo, particularmente conteúdo que tende a se tornar menos popular com o tempo. Exemplos incluem conteúdo gerado pelo usuário, como vídeo, fotos ou arte; ativos de e-commerce, como fotos e vídeos de produtos; e conteúdo relacionado a notícias e eventos que pode repentinamente encontrar nova popularidade.

O Amazon CloudFront é a resposta certa porque podemos colocá-lo na frente do nosso grupo de dimensionamento automático e aproveitar um recurso de cache global que nos ajudará a distribuir o conteúdo de forma confiável com custos drasticamente reduzidos (o ASG não precisará ser dimensionado tanto).

Pergunta 62

Uma empresa de compartilhamento de caronas quer usar uma tabela do Amazon DynamoDB para armazenamento de dados. A tabela não será usada durante as horas da noite, enquanto o tráfego de leitura e gravação geralmente será imprevisível durante as horas do dia. Quando picos de tráfego ocorrem, eles acontecem muito rapidamente.

Qual das seguintes opções você recomendaria como a solução mais adequada?

R: Configurar a tabela Amazon DynamoDB no modo de capacidade sob demanda

Opção correta:

Configurar a tabela Amazon DynamoDB no modo de capacidade sob demanda

O Amazon DynamoDB tem dois modos de capacidade de leitura/gravação para processar leituras e gravações em suas tabelas:

Sob demanda

Provisionado (padrão, elegível para nível gratuito)

O Amazon DynamoDB on-demand é uma opção de cobrança flexível capaz de atender milhares de solicitações por segundo sem planejamento de capacidade. O DynamoDB on-demand oferece preços de pagamento por solicitação para solicitações de leitura e gravação, para que você pague apenas pelo que usar.

O modo sob demanda é uma boa opção se alguma das seguintes condições for verdadeira:

Você cria novas tabelas com cargas de trabalho desconhecidas.

Você tem tráfego de aplicativos imprevisível.

Você prefere a facilidade de pagar apenas pelo que usa.

Se você escolher o modo provisionado, especifique o número de leituras e gravações por segundo que você precisa para seu aplicativo. Você pode usar o dimensionamento automático para ajustar a capacidade provisionada da sua tabela automaticamente em resposta a alterações de tráfego. Isso ajuda você a governar seu uso do DynamoDB para permanecer em ou abaixo de uma taxa de solicitação definida para obter previsibilidade de custo.

O modo provisionado é uma boa opção se alguma das seguintes condições for verdadeira:

Você tem tráfego de aplicativos previsível.

Você executa aplicativos cujo tráfego é consistente ou aumenta gradualmente.

Você pode prever requisitos de capacidade para controlar custos.

Com o on-demand, o Amazon DynamoDB aloca capacidade instantaneamente conforme necessário. Não há conceito de capacidade provisionada e não há atraso esperando por limites do Amazon CloudWatch ou atualizações de tabela subsequentes. O on-demand é ideal para cargas de trabalho explosivas, novas ou imprevisíveis cujo tráfego pode aumentar em segundos ou minutos, e quando a capacidade subprovisionada impactaria a experiência do usuário. O on-demand é uma solução perfeita se sua equipe estiver migrando para um ambiente NoOps ou sem servidor.

O caso de uso fornecido afirma claramente que, quando os picos de tráfego ocorrem, eles acontecem muito rapidamente, o que implica um padrão de tráfego imprevisível; portanto, o modo de capacidade sob demanda é a opção correta para o caso de uso fornecido.

Pergunta 63

Você desenvolveu uma nova API REST aproveitando os serviços de banco de dados Amazon API Gateway, AWS Lambda e Amazon Aurora. A maior parte da carga de trabalho no site é de leitura pesada. Os dados raramente mudam e é aceitável fornecer aos usuários dados desatualizados por cerca de 24 horas. Recentemente, o site tem enfrentado alta carga e os custos incorridos no banco de dados Aurora têm sido muito altos.

Como você pode reduzir facilmente os custos e, ao mesmo tempo, melhorar o desempenho, com mudanças mínimas?

R: Habilitar cache do Amazon API Gateway

Opção correta:

Habilitar cache do Amazon API Gateway

O Amazon API Gateway é um serviço totalmente gerenciado que facilita para os desenvolvedores criar, publicar, manter, monitorar e proteger APIs em qualquer escala. As APIs atuam como a "porta de entrada" para que os aplicativos acessem dados, lógica de negócios ou funcionalidade dos seus serviços de backend. Usando o API Gateway, você pode criar APIs RESTful e APIs WebSocket que permitem aplicativos de comunicação bidirecional em tempo real. O API Gateway oferece suporte a cargas de trabalho em contêineres e sem servidor, bem como aplicativos da Web.

Você pode habilitar o cache da Amazon API no Amazon API Gateway para armazenar em cache as respostas do seu endpoint. Com o cache, você pode reduzir o número de chamadas feitas para o seu endpoint e também melhorar a latência das solicitações para sua API. Quando você habilita o cache para um estágio, o API Gateway armazena em cache as respostas do seu endpoint por um período de tempo de vida (TTL) especificado, em segundos. O Amazon API Gateway responde à solicitação procurando a resposta do endpoint no cache em vez de solicitar seu endpoint. O valor TTL padrão para o cCorpo do textoache da API é 300 segundos. O valor TTL máximo é 3600 segundos. TTL=0 significa que o cache está desabilitado. Usar o recurso de cache do API Gateway é a resposta para o caso de uso, pois podemos aceitar dados obsoletos por cerca de 24 horas.

Pergunta 64

O Amazon Route 53 está configurado para rotear tráfego para dois nós do Network Load Balancer pertencentes a duas Zonas de Disponibilidade (AZs): AZ-A e AZ-B. O balanceamento de carga entre

zonas está desabilitado. AZ-A tem quatro destinos e AZ-B tem seis destinos.

Qual das afirmações abaixo é verdadeira sobre a distribuição de tráfego para as instâncias de destino do Amazon Route 53?

R: Cada um dos quatro alvos AZ-A recebe 12,5% do tráfego

Opção correta:

Cada um dos quatro alvos AZ-A recebe 12,5% do tráfego

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 (AZs) habilitadas. Quando o balanceamento de carga entre zonas está desabilitado, cada nó do balanceador de carga distribui o tráfego somente entre os destinos registrados em sua Zona de Disponibilidade (AZ).

O Amazon Route 53 distribuirá o tráfego de forma que cada nó do balanceador de carga receba 50% do tráfego dos clientes.

Se o balanceamento de carga entre zonas estiver desabilitado: 1. Cada um dos quatro destinos em AZ-

A recebe 12,5% do tráfego. 2. Cada um dos seis destinos em AZ-B recebe 8,3% 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 (AZ).

Pergunta 65

Como ArquCorpo do textouiteto de Soluções, você tem a tarefa de projetar uma aplicação distribuída que será executada em várias instâncias do Amazon EC2. Essa aplicação precisa ter o disco local de mais alto desempenho para armazenar dados em cache. Além disso, os dados são copiados por meio de um mecanismo de replicação do Amazon EC2 para o EC2. É aceitável que a instância perca seus dados ao ser interrompida ou encerrada.

Qual solução de armazenamento você recomenda?

R: Loja de Instâncias

Opção correta:

Loja de Instâncias

Um armazenamento de instâncias fornece armazenamento temporário em nível de bloco para sua instância. Esse armazenamento está localizado em discos fisicamente conectados ao computador host. O armazenamento de instâncias é ideal para o armazenamento temporário de informações que mudam com frequência, como buffers, caches, dados temporários e outros conteúdos temporários, ou para dados replicados em uma frota de instâncias, como um pool de servidores web com balanceamento de carga.

Os volumes de armazenamento de instâncias são incluídos como parte do custo de uso da instância. Alguns tipos de instância usam unidades de estado sólido (SSD) baseadas em NVMe ou SATA para oferecer alto desempenho de E/S aleatória. Essa é uma boa opção quando você precisa de armazenamento com latência muito baixa, mas não precisa que os dados persistam após o encerramento da instância.