Pergunta 1

Uma empresa de Big Data deseja otimizar seu processo diário de Extração-Transformação-Carregamento (ETL), que migra e transforma dados de seu data lake baseado no Amazon S3 para um cluster do Amazon Redshift. A equipe deseja gerenciar essa tarefa diária em um ambiente sem servidor.

Qual serviço da AWS é mais adequado para gerenciar esse processo sem a necessidade de configurar ou gerenciar os recursos de computação subjacentes?

R: Cola AWS

Opção correta:

Cola AWS

O AWS Glue fornece um serviço de ETL gerenciado executado em um ambiente Apache Spark sem servidor. Isso permite que você se concentre em sua tarefa de ETL e não se preocupe em configurar e gerenciar os recursos computacionais subjacentes. O AWS Glue adota uma abordagem que prioriza os dados e permite que você se concentre nas propriedades e na manipulação dos dados para transformá-los em um formato no qual você possa obter insights de negócios. Ele fornece um catálogo de dados integrado que disponibiliza metadados para ETL, bem como para consultas via Amazon Athena e Amazon Redshift Spectrum.

Crie um catálogo unificado para encontrar dados em vários armazenamentos de dados usando o AWS

O AWS Glue automatiza grande parte do esforço necessário para a integração de dados. O AWS Glue rastreia suas fontes de dados, identifica formatos de dados e sugere esquemas para armazená-los. Ele gera automaticamente o código para executar suas transformações de dados e processos de carregamento. Você pode usar o AWS Glue para executar e gerenciar facilmente milhares de tarefas de ETL ou para combinar e replicar dados em vários repositórios de dados usando SQL.

O AWS Glue é executado em um ambiente sem servidor. Não há infraestrutura para gerenciar, e o AWS Glue provisiona, configura e dimensiona os recursos necessários para executar seus trabalhos de integração de dados. Você paga apenas pelos recursos que seus trabalhos utilizam durante a execução.

O AWS Glue é a opção certa, pois a empresa está buscando um serviço ETL gerenciado sem ter a sobrecarga de configurar, manter ou gerenciar quaisquer servidores.

Pergunta 2

Uma empresa de serviços financeiros armazena dados confidenciais em um bucket do Amazon Simple Storage Service (S3). As diretrizes de conformidade exigem que os arquivos sejam armazenados com criptografia do lado do servidor. A criptografia utilizada deve ser Advanced Encryption Standard (AES-256) e a empresa não deseja gerenciar as chaves de criptografia.

Qual das seguintes opções representa a solução com melhor custo-benefício para o caso de uso em questão?

R: Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Opção correta:

Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Usando a Criptografia do Lado do Servidor com Chaves Gerenciadas pelo Amazon S3 (SSE-S3), cada objeto é criptografado com uma chave exclusiva, empregando criptografia multifator robusta. Como proteção adicional, a criptografia da própria chave é feita com uma chave mestra que é rotacionada regularmente. A criptografia do lado do servidor do Amazon S3 utiliza uma das cifras de bloco mais robustas disponíveis, o Advanced Encryption Standard (AES-256) de 256 bits, para criptografar seus dados. Não há taxas adicionais para usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Pergunta 3

Um consultor de segurança está projetando uma solução para uma empresa que deseja fornecer aos desenvolvedores contas individuais da AWS por meio do AWS Organizations, mantendo os controles de segurança padrão. Como os desenvolvedores individuais terão acesso root às suas próprias contas, o consultor deseja garantir que a configuração obrigatória do AWS CloudTrail aplicada às novas contas de desenvolvedor não seja modificada.

Qual das seguintes ações atende aos requisitos fornecidos?

R: Configure uma política de controle de serviço (SCP) que proíba alterações no AWS CloudTrail e anexe-a às contas de desenvolvedor

Opção correta:

Configure uma política de controle de serviço (SCP) que proíba alterações no AWS CloudTrail e anexe-a às contas de desenvolvedor

A Política de Controle de Serviço (SCP) é um tipo de política organizacional que você pode usar para gerenciar permissões na sua organização. As SCPs oferecem controle central sobre o máximo de permissões disponíveis para todas as contas da sua organização. Elas ajudam a garantir que suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização.

Um SCP restringe permissões para usuários e funções do IAM em contas de membro, incluindo o usuário raiz da conta de membro. Qualquer conta tem apenas as permissões concedidas por todos os pais acima dela. Se uma permissão for bloqueada em qualquer nível acima da conta, seja implicitamente (por não ser incluída em uma declaração de política de permissão) ou explicitamente (por ser incluída em uma declaração de política de negação), um usuário ou função na conta afetada não poderá usar essa permissão, mesmo que o administrador da conta tenha anexado a política do IAM "AdministratorAccess" com permissões / ao usuário.

SCPs não afetam usuários ou funções na conta de gerenciamento. Eles afetam apenas as contas de membros da sua organização.

Pergunta 4

Uma empresa possui arquivos de mídia que precisam ser compartilhados internamente. Os usuários são primeiro autenticados usando o Active Directory e, em seguida, acessam os arquivos em uma plataforma Microsoft Windows. O gerente de engenharia deseja manter as mesmas permissões de usuário, mas deseja que a empresa migre a camada de armazenamento para a Nuvem AWS, pois a empresa está atingindo o limite de capacidade de armazenamento na infraestrutura local.

O que um arquiteto de soluções deve recomendar para atender a esse requisito?

R: Configure o Amazon FSx para o Windows File Server e mova todos os arquivos de mídia

Opção correta:

Configure o Amazon FSx para o Windows File Server e mova todos os arquivos de mídia

O Amazon FSx para Windows File Server oferece armazenamento de arquivos totalmente gerenciado, altamente confiável e escalável, acessível através do protocolo SMB (Server Message Block), padrão do setor. Ele é baseado no Windows Server e oferece uma ampla gama de recursos administrativos, como cotas de usuários, restauração de arquivos para usuários finais e integração com o Microsoft Active Directory (AD). Para suportar uma ampla gama de cargas de trabalho, o Amazon FSx oferece altos níveis de throughput e IOPS, além de latências consistentes abaixo de milissegundos.

O armazenamento de arquivos do Amazon FSx pode ser acessado a partir de instâncias e dispositivos de computação Windows, Linux e macOS executados na AWS ou no local. Milhares de instâncias e dispositivos de computação podem acessar um sistema de arquivos simultaneamente. O Amazon FSx para Windows File Server oferece suporte à integração com o Microsoft Active Directory (AD), permitindo que as mesmas permissões de usuário e credenciais de acesso sejam usadas para acessar os arquivos no FSx Windows File Server.

Pergunta 5

Uma empresa de análise de big data está buscando arquivar os dados locais em um sistema de armazenamento de arquivos compatível com POSIX na Nuvem AWS. Os dados arquivados seriam acessados por apenas uma semana por ano.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você recomendaria como a solução com o MELHOR custo-benefício?

R: Acesso pouco frequente do Amazon EFS

Opção correta:

Acesso pouco frequente do Amazon EFS

O Amazon Elastic File System (Amazon EFS) oferece um sistema de arquivos NFS simples, escalável, totalmente gerenciado e elástico para uso com serviços da Nuvem AWS e recursos locais. O Amazon EFS Infrequent Access (EFS IA) é uma classe de armazenamento que oferece preço/desempenho otimizados para arquivos que não são acessados diariamente, com preços de armazenamento até 92% mais baixos em comparação com o Amazon EFS Standard. A classe de armazenamento EFS IA custa apenas US$ 0,025/GB/mês. Para começar a usar o EFS IA, basta habilitar o EFS Lifecycle Management para o seu sistema de arquivos, selecionando uma política de ciclo de vida que atenda às suas necessidades.

Como funciona o acesso pouco frequente do Amazon EFS:

Pergunta 6

Um aplicativo em execução em uma instância do Amazon EC2 precisa acessar uma tabela do Amazon DynamoDB na mesma conta da AWS.

Qual das seguintes soluções um arquiteto de soluções deve configurar para as permissões necessárias?

R: Configure uma função de serviço do IAM com as permissões apropriadas para permitir acesso à tabela do Amazon DynamoDB. Configure um perfil de instância para atribuir essa função do IAM à instância do Amazon EC2.

Opção correta:

Configure uma função de serviço do IAM com as permissões apropriadas para permitir acesso à tabela do Amazon DynamoDB. Configure um perfil de instância para atribuir essa função do IAM à instância do Amazon EC2.

Uma função de serviço é uma função do IAM que um serviço assume para executar ações em seu nome. As funções de serviço fornecem acesso apenas dentro da sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador do IAM pode criar, modificar e excluir uma função de serviço dentro do IAM. Ao criar a função de serviço, você a define `trusted entity` na definição. Se você for usar a função com o Amazon EC2 ou outro serviço da AWS que utilize o Amazon EC2, será necessário armazená-la em um perfil de instância. Um perfil de instância é um contêiner para uma função que pode ser anexado a uma instância do Amazon EC2 quando iniciada. Um perfil de instância pode conter apenas uma função, e esse limite não pode ser aumentado. Se você criar a função usando o Console de Gerenciamento da AWS, o perfil de instância será criado para você com o mesmo nome da função.

Pergunta 7

Uma empresa está enfrentando problemas de estabilidade com seu cluster de corretores de mensagens RabbitMQ autogerenciados e agora quer explorar uma solução alternativa na AWS.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você recomendaria para fornecer suporte para uma migração rápida e fácil do RabbitMQ?

R: Amazon MQ

Opção correta:

Amazon MQ
O Amazon MQ é um serviço gerenciado de corretor de mensagens para o Apache ActiveMQ que facilita a configuração e a operação de corretores de mensagens na nuvem. Os corretores de mensagens permitem que diferentes sistemas de software – frequentemente 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. Portanto, esta é a opção correta.

Pergunta 8

Uma empresa está implantando uma aplicação web acessível publicamente. Para isso, a equipe de engenharia projetou a VPC com uma sub-rede pública e uma sub-rede privada. A aplicação será hospedada em várias instâncias do Amazon EC2 em um grupo de Auto Scaling. A equipe também deseja que a terminação do Transport Layer Security (TLS) seja descarregada das instâncias do Amazon EC2.

Qual solução um arquiteto de soluções deve implementar para atender a esses requisitos da maneira mais segura?

Configure um balanceador de carga de rede na sub-rede pública. Crie um grupo de dimensionamento automático na sub-rede privada e associe-o ao balanceador de carga de rede.

Opção correta:

Configure um balanceador de carga de rede na sub-rede pública. Crie um grupo de dimensionamento automático na sub-rede privada e associe-o ao balanceador de carga de rede.
Um balanceador de carga serve como ponto de contato único para os clientes. O balanceador de carga distribui o tráfego de entrada entre vários destinos, como instâncias do Amazon EC2. Isso aumenta a disponibilidade da sua aplicação. Você adiciona um ou mais ouvintes ao seu balanceador de carga.
Com um Balanceador de Carga de Rede, você pode transferir a descriptografia/criptografia do tráfego TLS (Transport Layer Security) dos seus servidores de aplicativos para o Balanceador de Carga de Rede, o que ajuda a otimizar o desempenho dos seus servidores de aplicativos de back-end, mantendo suas cargas de trabalho seguras. Além disso, os Balanceadores de Carga de Rede preservam o IP de origem dos clientes para os aplicativos de back-end, enquanto encerram o TLS (Transport Layer Security) no balanceador de carga.
Um grupo de Auto Scaling contém uma coleção de instâncias do Amazon EC2 que são tratadas como um agrupamento lógico para fins de dimensionamento 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 dimensionamento. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto o dimensionamento automático são as principais funcionalidades do serviço Amazon EC2 Auto Scaling.
O NLB precisa ser acessível pela internet e, portanto, precisa estar em uma sub-rede pública, atuando como um único ponto de contato para todo o tráfego de entrada. O NLB encaminhará o tráfego de entrada para as instâncias do Amazon EC2 gerenciadas pelo ASG na sub-rede privada.
Alerta de exame:
Observe que o Application Load Balancer também oferece suporte ao descarregamento de Segurança da Camada de Transporte (TLS). O Classic Load Balancer oferece suporte ao descarregamento de SSL.

Pergunta 9

Uma empresa de consultoria em Big Data executa grandes cargas de trabalho distribuídas e replicadas no data center local. A empresa agora deseja mover essas cargas de trabalho para instâncias do Amazon EC2 usando o recurso de grupos de posicionamento e deseja minimizar falhas de hardware

correlacionadas.

Qual das opções a seguir representa a configuração correta do grupo de posicionamento para o requisito fornecido?

R: Grupos de posicionamento de partição

Opção correta:

Grupos de posicionamento de partição

Grupos de posicionamento de partições ajudam a reduzir a probabilidade de falhas de hardware correlacionadas para sua aplicação. Ao usar grupos de posicionamento de partições, o Amazon EC2 divide cada grupo em segmentos lógicos chamados partições. O Amazon EC2 garante que cada partição dentro de um grupo de posicionamento tenha seu próprio conjunto de racks. Cada rack tem sua própria rede e fonte de alimentação. Nenhuma das duas partições dentro de um grupo de posicionamento compartilhe os mesmos racks, permitindo isolar o impacto de uma falha de hardware em sua aplicação.

A imagem a seguir é uma representação visual simples de um grupo de posicionamento de partições em uma única Zona de Disponibilidade. Ela mostra instâncias colocadas em um grupo de posicionamento de partições com três partições: Partição 1, Partição 2 e Partição 3. Cada partição compreende várias instâncias. As instâncias em uma partição não compartilham racks com as instâncias nas outras partições, permitindo que você limite o impacto de uma única falha de hardware apenas à partição associada.

Grupos de posicionamento de partições podem ser usados para implantar grandes cargas de trabalho distribuídas e replicadas, como HDFS, HBase e Cassandra, em racks distintos. Ao iniciar instâncias em um grupo de posicionamento de partições, o Amazon EC2 tenta distribuí-las uniformemente entre o número de partições especificado. Você também pode iniciar instâncias em uma partição específica para ter mais controle sobre onde elas serão colocadas.

Um grupo de posicionamento de partições pode ter partições em várias Zonas de Disponibilidade na mesma Região. Um grupo de posicionamento de partições pode ter no máximo sete partições por Zona de Disponibilidade. O número de instâncias que podem ser iniciadas em um grupo de posicionamento de partições é limitado apenas pelos limites da sua conta.

Pergunta 10

A equipe de DevOps de uma empresa de e-commerce implantou uma frota de instâncias do Amazon EC2 em um grupo de Auto Scaling (ASG). As instâncias sob o ASG abrangem duas Zonas de Disponibilidade (AZ) na us-east-1região. Todas as solicitações recebidas são gerenciadas por um Balanceador de Carga de Aplicativos (ALB), que as encaminha para as instâncias do Amazon EC2 sob o Grupo de Auto Scaling. Como parte de um teste, duas instâncias (instâncias 1 e 2, pertencentes à AZ A) foram encerradas manualmente pela equipe de DevOps, causando desequilíbrio de recursos nas Zonas de Disponibilidade (AZ). Mais tarde naquele dia, outra instância (pertencente à AZ B) foi detectada como não íntegra pela verificação de integridade do Balanceador de Carga de Aplicativos.

Você consegue identificar os resultados corretos para esses eventos? (Selecione dois)

R: O Amazon EC2 Auto Scaling cria uma nova atividade de escalonamento para encerrar a instância com problemas de integridade e, em seguida, a encerra. Posteriormente, outra atividade de escalonamento inicia uma nova instância para substituir a instância encerrada.

R: Como os recursos estão desbalanceados nas Zonas de Disponibilidade, o Amazon EC2 Auto Scaling compensará rebalanceando as Zonas de Disponibilidade. Durante o rebalanceamento, o Amazon EC2 Auto Scaling inicia novas instâncias antes de encerrar as antigas, para que o rebalanceamento não comprometa o desempenho ou a disponibilidade do seu aplicativo.

Opções corretas:

Como os recursos estão desbalanceados nas Zonas de Disponibilidade, o Amazon EC2 Auto Scaling compensará rebalanceando as Zonas de Disponibilidade. Durante o rebalanceamento, o Amazon EC2 Auto Scaling inicia novas instâncias antes de encerrar as antigas, para que o rebalanceamento não comprometa o desempenho ou a disponibilidade do seu aplicativo.

O Amazon EC2 Auto Scaling ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga do seu aplicativo. Você cria coleções de instâncias do 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. Ações como alterar as Zonas de Disponibilidade (AZ) do seu grupo ou encerrar ou desanexar instâncias explicitamente podem fazer com que o grupo de Auto Scaling fique desbalanceado entre as Zonas de Disponibilidade. O Amazon EC2 Auto Scaling compensa rebalanceando as Zonas de Disponibilidade.
Ao rebalancear, o Amazon EC2 Auto Scaling inicia novas instâncias antes de encerrar as antigas, para que o rebalanceamento não comprometa o desempenho ou a disponibilidade do seu aplicativo. Portanto, esta opção está correta.

O Amazon EC2 Auto Scaling cria uma nova atividade de escalonamento para encerrar a instância com problemas de integridade e, em seguida, a encerra. Posteriormente, outra atividade de escalonamento inicia uma nova instância para substituir a instância encerrada.
No entanto, a atividade de escalonamento do Auto Scaling funciona em uma sequência diferente da atividade de rebalanceamento. O Auto Scaling cria uma nova atividade de escalonamento para encerrar a instância com problemas e, em seguida, a encerra. Posteriormente, outra atividade de escalonamento inicia uma nova instância para substituir a instância encerrada.

Pergunta 11

Durante uma análise, uma equipe de segurança sinalizou preocupações sobre uma instância do Amazon EC2 que consulta endereços IP usados para mineração de criptomoedas. A instância do Amazon EC2 não hospeda nenhum aplicativo autorizado relacionado à mineração de criptomoedas.
Qual serviço da AWS pode ser usado para proteger as instâncias do Amazon EC2 desse comportamento não autorizado no futuro?
Amazon GuardDuty

Opção correta:

Amazon GuardDuty
O Amazon GuardDuty monitora continuamente comportamentos maliciosos ou não autorizados para ajudar a proteger seus recursos da AWS, incluindo suas contas e chaves de acesso. O Amazon GuardDuty identifica qualquer atividade incomum ou não autorizada, como mineração de criptomoedas ou implantações de infraestrutura em uma região que nunca foi utilizada. Com tecnologia de inteligência contra ameaças e aprendizado de máquina, o GuardDuty está em constante evolução para ajudar você a proteger seu ambiente da AWS.
A descoberta de criptomoedas expande a capacidade do serviço de detectar instâncias do Amazon EC2 que consultam endereços IP associados à atividade relacionada a criptomoedas. O tipo de descoberta é: CryptoCurrency:EC2/BitcoinTool.B, CryptoCurrency:EC2/BitcoinTool.B!DNS.
Esta descoberta informa que a instância do Amazon EC2 listada em seu ambiente AWS está consultando um nome de domínio associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda e sistema de pagamento digital mundial que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoin e é muito procurado por agentes de ameaças.
Se você usa a instância do Amazon EC2 para minerar ou gerenciar criptomoedas, ou se esta instância estiver envolvida em alguma atividade de blockchain, esta descoberta pode representar uma atividade esperada para o seu ambiente. Se este for o caso no seu ambiente AWS, a AWS recomenda que você configure uma regra de supressão para esta descoberta.

Pergunta 12

Uma equipe de desenvolvimento quer garantir que todos os objetos enviados para um bucket do Amazon S3 sejam criptografados?
Qual das seguintes opções representa a solução correta?

R: Configure a política de bucket para negar se o PutObject não tiver um cabeçalho x-amz-server-side-encryption definido

Opção correta:

Configure a política de bucket para negar se o PutObject não tiver um cabeçalho x-amz-server-side-encryption definido
O Amazon S3 criptografa seus dados no nível do objeto à medida que grava em discos nos data centers da AWS e os descriptografa para você quando você os acessa. Você pode criptografar objetos usando criptografia do lado do cliente ou criptografia do lado do servidor. A criptografia do lado do cliente ocorre quando um objeto é criptografado antes de você carregá-lo no Amazon S3, e as chaves não são gerenciadas pela AWS. Com a criptografia do lado do servidor, a Amazon gerencia as chaves de uma das três maneiras:

- Criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C).
- SSE-S3.
- SSE-KMS.

A criptografia do lado do servidor envolve a criptografia de dados em repouso — ou seja, o Amazon S3 criptografa seus dados no nível do objeto enquanto os grava em discos em seus data centers e os descriptografa para você quando você os acessa. Desde que você autentique sua solicitação e tenha permissões de acesso, não há diferença na forma como você acessa objetos criptografados ou não criptografados.
Para criptografar um objeto no momento do upload, você precisa adicionar um cabeçalho chamado x-amz-server-side-encryption à solicitação para informar ao S3 para criptografar o objeto usando SSE-C, SSE-S3 ou SSE-KMS.
Para aplicar a criptografia de objetos, crie uma política de bucket do Amazon S3 que negue qualquer solicitação Put do S3 que não inclua o cabeçalho x-amz-server-side-encryption. Há dois valores possíveis para o cabeçalho x-amz-server-side-encryption: AES256, que informa ao S3 para usar chaves gerenciadas pelo S3, e aws:kms, que informa ao Amazon S3 para usar chaves gerenciadas pelo AWS KMS.

Pergunta 13

Uma equipe de desenvolvimento notou que uma das instâncias do Amazon EC2 foi configurada incorretamente com o atributo 'DeleteOnTermination' definido como True para seu volume raiz do EBS.
`Como arquiteto de soluções, você pode sugerir uma maneira de desabilitar esse sinalizador enquanto a instância ainda estiver em execução?`
- Defina o `DeleteOnTermination` atributo como False usando a linha de comando

Opção correta:

Quando uma instância é encerrada, o valor do atributo DeleteOnTermination para cada volume EBS anexado determina se o volume deve ser preservado ou excluído. Por padrão, o atributo DeleteOnTermination é definido como True para o volume raiz e como False para todos os outros tipos de volume.
Defina o `DeleteOnTermination` atributo como False usando a linha de comando
Se a instância já estiver em execução, você pode definir `DeleteOnTermination` como False usando a linha de comando.

Pergunta 14

Uma empresa de comércio eletrônico utiliza o banco de dados MySQL do Amazon RDS para armazenar os dados. O departamento de análise da empresa executa seus relatórios no mesmo banco de dados. A equipe de engenharia notou um desempenho lento no banco de dados durante o processo de geração de relatórios analíticos.

Como Arquiteto de Soluções Certificado pela AWS - Associado, qual das seguintes opções você sugeriria como a solução MAIS econômica para melhorar o desempenho?

R: Crie uma réplica de leitura com a mesma capacidade de computação e armazenamento que a primária. Direcione as consultas de relatórios para execução na réplica de leitura.

Opção correta:

Crie uma réplica de leitura com a mesma capacidade de computação e armazenamento que a primária. Direcione as consultas de relatórios para execução na réplica de leitura.
O Amazon RDS utiliza a funcionalidade de replicação integrada dos mecanismos de banco de dados MariaDB, Microsoft SQL Server, MySQL, Oracle e PostgreSQL para criar um tipo especial de instância de banco de dados, chamada réplica de leitura, a partir de uma instância de banco de dados de origem. A instância de banco de dados de origem se torna a instância de banco de dados primária. As atualizações feitas na instância de banco de dados primária são copiadas de forma assíncrona para a réplica de leitura. Você pode reduzir a carga na sua instância de banco de dados primária roteando consultas de leitura dos seus aplicativos para a réplica de leitura.

Você pode usar réplicas de leitura para melhorar o desempenho do seu banco de dados MySQL do Amazon RDS manipulando relatórios comerciais ou cenários de armazenamento de dados nos quais você pode querer que consultas de relatórios comerciais sejam executadas na sua réplica de leitura, em vez da sua instância de banco de dados de produção.
Você pode criar até cinco réplicas de leitura a partir de uma instância de banco de dados. Para que a replicação funcione de forma eficaz, cada réplica de leitura deve ter a mesma quantidade de recursos de computação e armazenamento que a instância do banco de dados de origem. Se você dimensionar a instância do banco de dados de origem, dimensione também as réplicas de leitura

Pergunta 15

Uma aplicação de e-commerce utiliza um banco de dados relacional que executa diversas consultas que realizam junções em múltiplas tabelas. A equipe de desenvolvimento constatou que essas consultas são lentas e caras, sendo, portanto, boas candidatas para armazenamento em cache. A aplicação precisa utilizar um serviço de cache que suporte multithreading.

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

R: Amazon ElastiCache para Memcached

Opção correta:

Amazon ElastiCache para Memcached
O Amazon ElastiCache é um serviço web que facilita a implantação, a operação e o escalonamento de um armazenamento de dados e cache na memória na nuvem. O serviço melhora o desempenho de aplicações web, permitindo que você recupere informações de armazenamentos de dados na memória rápidos e gerenciados, em vez de depender inteiramente de bancos de dados mais lentos baseados em disco.
O Memcached é um repositório de chave-valor distribuído e de código aberto na memória que pode recuperar dados em milissegundos. Armazenar informações do site em cache com o Memcached pode ajudar você a melhorar o desempenho e a escalabilidade do seu site, controlando custos.
Escolha Memcached se o seguinte se aplicar a você:
Você precisa do modelo mais simples possível.
Você precisa executar nós grandes com vários núcleos ou threads (suporte para multithreading).
Você precisa ter a capacidade de escalar horizontalmente e horizontalmente, adicionando e removendo nós conforme a demanda no seu sistema aumenta e diminui.
Você precisa armazenar objetos em cache.

Pergunta 16

Uma startup utiliza uma frota de servidores Amazon EC2 para gerenciar seu aplicativo de CRM. Esses servidores Amazon EC2 estão por trás do Elastic Load Balancing (ELB). Quais das seguintes configurações NÃO são permitidas para o Elastic Load Balancing?

R: Use o Elastic Load Balancing para distribuir o tráfego para quatro instâncias do Amazon EC2. Duas dessas instâncias estão implantadas na Zona de Disponibilidade A da região us-east-1 e as outras duas instâncias estão implantadas na Zona de Disponibilidade B da `us-west-1` região.

Opção correta:

Use o Elastic Load Balancing para distribuir o tráfego para quatro instâncias do Amazon EC2. Duas dessas instâncias estão implantadas na Zona de Disponibilidade A da região us-east-1 e as outras duas instâncias estão implantadas na Zona de Disponibilidade B da `us-west-1` região.

O Elastic Load Balancer distribui automaticamente o tráfego de entrada entre vários destinos – instâncias do Amazon EC2, contêineres, endereços IP e funções Lambda – em várias Zonas de Disponibilidade e garante que apenas destinos íntegros recebam tráfego. O ELB não pode distribuir o tráfego de entrada para destinos implantados em regiões diferentes. Esta configuração NÃO é permitida para o Elastic Load Balancer e, portanto, esta é a opção correta.

Pergunta 17

Como Arquiteto de Soluções, você configurou um banco de dados em uma única instância do Amazon EC2 que possui um volume do Amazon EBS do tipo gp2. Atualmente, você tem 300 gigabytes de espaço no dispositivo gp2. A instância do Amazon EC2 é do tipo m5.large. O desempenho do banco de dados tem sido ruim recentemente e, ao analisar o Amazon CloudWatch, você percebe que o IOPS no volume do Amazon EBS está atingindo o limite. O tamanho do disco do banco de dados não deve ser alterado devido a um problema de licenciamento.

Como você soluciona esse problema?

R: Converter o volume gp2 em um io1

Pare o agente Amazon CloudWatch para melhorar o desempenho

Opção correta:

O Amazon EBS oferece os seguintes 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

Converter o volume gp2 em um io1
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.
A única solução é converter o volume para um volume io1. Isso nos permitirá manter o mesmo tamanho de disco e, ao mesmo tempo, aumentar o IOPS desse volume de forma independente.

Pergunta 18

Uma startup deseja criar uma arquitetura de alta disponibilidade para sua aplicação multicamadas. Atualmente, a startup gerencia uma única instância do Amazon EC2, além de uma única instância do

banco de dados MySQL do Amazon RDS. A startup contratou você como Arquiteto de Soluções Certificado pela AWS - Associado para desenvolver uma solução que atenda a esses requisitos, minimizando o esforço de manutenção da infraestrutura subjacente.

O que você recomendaria?

R: Crie um grupo de Auto-Scaling com uma capacidade desejada de um total de duas instâncias do Amazon EC2 em duas Zonas de Disponibilidade. Configure um Application Load Balancer com um grupo-alvo dessas instâncias do Amazon EC2. Configure o banco de dados MySQL do Amazon RDS em uma configuração multi-AZ.

Opção correta:

Crie um grupo de Auto-Scaling com uma capacidade desejada de um total de duas instâncias do Amazon EC2 em duas Zonas de Disponibilidade. Configure um Application Load Balancer com um grupo-alvo dessas instâncias do Amazon EC2. Configure o banco de dados MySQL do Amazon RDS em uma configuração multi-AZ.

O Amazon EC2 Auto Scaling é um serviço totalmente gerenciado projetado para iniciar ou encerrar instâncias do Amazon EC2 automaticamente para ajudar a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga do seu aplicativo.

O Application Load Balancer distribui automaticamente o tráfego de entrada entre vários destinos, como instâncias do Amazon EC2, contêineres e endereços IP, em uma ou mais Zonas de Disponibilidade. Ele monitora a integridade dos seus destinos registrados e encaminha o tráfego apenas para os destinos íntegros.

Em uma implantação multi-AZ, o Amazon RDS provisiona e mantém automaticamente uma réplica "standby" síncrona em uma Zona de Disponibilidade diferente. As atualizações da sua Instância de Banco de Dados são replicadas de forma síncrona entre as Zonas de Disponibilidade para a standby, mantendo ambas sincronizadas e protegendo as atualizações mais recentes do seu banco de dados contra falhas na instância de Banco de Dados.

Para criar uma arquitetura de alta disponibilidade para o caso de uso fornecido, você precisa configurar um grupo de dimensionamento automático com uma capacidade desejada de um total de duas instâncias do Amazon EC2 em duas zonas de disponibilidade e, em seguida, apontar o Application Load Balancer para o grupo de destino que tem as instâncias do Amazon EC2.

Pergunta 19

Uma equipe tem cerca de 200 usuários, cada um com uma conta de usuário do IAM na AWS. Atualmente, todos eles têm acesso de leitura a um bucket do Amazon S3. A equipe quer que 50 deles tenham acesso de leitura e gravação aos buckets.

Como você pode fornecer acesso a esses usuários no menor tempo possível, com o mínimo de alterações?

R: Crie um grupo, anexe a política ao grupo e coloque os usuários no grupo

Opção correta:

Crie um grupo, anexe a política ao grupo e coloque os usuários no grupo

Um grupo do IAM é um conjunto de usuários do IAM. Você pode usar grupos para especificar permissões para um conjunto de usuários, o que pode facilitar o gerenciamento dessas permissões. Por exemplo, você pode ter um grupo chamado Administradores e atribuir a esse grupo os tipos de permissões que os administradores normalmente precisam. Qualquer usuário nesse grupo terá automaticamente as permissões atribuídas a ele. Se um novo usuário ingressar na sua organização e precisar ter

privilégios de administrador, você poderá atribuir as permissões apropriadas adicionando o usuário a esse grupo.
Aqui, criar um grupo, atribuir usuários a esse grupo e anexar políticas a esse grupo é a melhor maneira.

Pergunta 20

Um aplicativo de mídia social permite que os usuários carreguem fotos e realizem operações de edição de imagens. O aplicativo oferece duas classes de serviço: Pro e Lite. A equipe do produto deseja que as fotos enviadas por usuários Pro sejam processadas antes das enviadas por usuários Lite. As fotos são carregadas no Amazon S3 e as informações do trabalho são enviadas para o Amazon SQS.

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

R: Crie duas filas padrão do Amazon SQS: uma para a versão Pro e outra para a Lite. Configure instâncias do Amazon EC2 para priorizar a consulta da fila Pro em relação à Lite.

Opção correta:

Crie duas filas padrão do Amazon SQS: uma para a versão Pro e outra para a Lite. Configure instâncias do Amazon EC2 para priorizar a consulta da fila Pro em relação à Lite.
A AWS recomenda o uso de filas separadas para priorizar o trabalho. Portanto, para o caso de uso em questão, você precisa criar uma fila padrão do Amazon SQS para processar fotos de usuários profissionais e outra fila padrão do Amazon SQS para processar fotos de usuários lite. Em seguida, você pode configurar instâncias do Amazon EC2 para priorizar a consulta da fila profissional em vez da fila lite.

Pergunta 21

Uma empresa utiliza um aplicativo de relatórios local legado que opera em gigabytes de arquivos .json e representa anos de dados. O aplicativo legado não consegue lidar com o tamanho crescente dos arquivos .json. Novos arquivos .json são adicionados diariamente, de diversas fontes de dados, a um local de armazenamento local central. A empresa deseja continuar a oferecer suporte ao aplicativo legado. A empresa contratou você como arquiteto de soluções para desenvolver uma solução que possa gerenciar atualizações contínuas de dados do seu aplicativo local para o Amazon S3.

Qual das seguintes soluções você sugeriria para atender ao requisito fornecido?

R: Configure um gateway de arquivos local. Configure fontes de dados para gravar os arquivos .json no gateway de arquivos. Aponte o aplicativo de análise legado para o gateway de arquivos. O gateway de arquivos deve replicar os arquivos .json para o Amazon S3.

Opção correta:

Configure um gateway de arquivos local. Configure fontes de dados para gravar os arquivos .json no gateway de arquivos. Aponte o aplicativo de análise legado para o gateway de arquivos. O gateway de arquivos deve replicar os arquivos .json para o Amazon S3.
Um gateway de arquivos fornece uma solução simples para apresentar um ou mais buckets do Amazon S3 e seus objetos como um compartilhamento de arquivos NFS ou SMB montável para um ou mais clientes locais.
O gateway de arquivos é implantado como uma máquina virtual em ambientes VMware ESXi ou Microsoft Hyper-V locais, ou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) na AWS. O gateway de arquivos também pode ser implantado em data centers e escritórios remotos em um dispositivo de hardware do Storage Gateway. Quando implantado, o gateway de arquivos fornece uma conexão perfeita entre clientes NFS (v3.0 ou v4.1) ou SMB (v1 ou v2) locais — normalmente aplicativos — e buckets do Amazon S3 hospedados em uma determinada região da AWS. O gateway de arquivos utiliza um cache local de leitura/gravação para fornecer acesso de baixa latência aos

dados para clientes de compartilhamento de arquivos na mesma rede local (LAN) que o gateway de arquivos.
Um compartilhamento de bucket consiste em um compartilhamento de arquivos hospedado a partir de um gateway de arquivos em um único bucket do Amazon S3. O dispositivo de máquina virtual do gateway de arquivos atualmente suporta até 10 compartilhamentos de bucket.
Arquitetura do File Gateway:

Pergunta 22

Você deseja criar um índice dos seus arquivos no Amazon S3 usando o Amazon RDS PostgreSQL. Para criar esse índice, é necessário ler os primeiros 250 bytes de cada objeto no Amazon S3, que contêm alguns metadados sobre o conteúdo do arquivo em si. Há mais de 100.000 arquivos no seu bucket do S3, totalizando 50 terabytes de dados.

Como você pode construir esse índice de forma eficiente?

R: Crie um aplicativo que percorrerá o bucket S3, emitirá uma Busca de intervalo de bytes para os primeiros 250 bytes e armazenará essas informações no Amazon RDS

Opção correta:

Crie um aplicativo que percorrerá o bucket S3, emitirá uma Busca de intervalo de bytes para os primeiros 250 bytes e armazenará essas informações no Amazon RDS
O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho líderes do setor.
Usando o cabeçalho HTTP Range em uma solicitação GET Object, você pode buscar um intervalo de bytes de um objeto, transferindo apenas a parte especificada. Você pode usar conexões simultâneas com o Amazon S3 para buscar diferentes intervalos de bytes dentro do mesmo objeto. Isso ajuda a obter uma taxa de transferência agregada mais alta em comparação com uma única solicitação de objeto inteiro. Buscar intervalos menores de um objeto grande também permite que seu aplicativo melhore os tempos de repetição quando as solicitações são interrompidas.
Uma solicitação de intervalo de bytes é uma maneira perfeita de obter o início de um arquivo e garantir a eficiência durante a varredura do bucket do Amazon S3. Portanto, esta é a opção correta.

Pergunta 23

O aplicativo de streaming em tempo real de uma empresa está sendo executado na AWS. À medida que os dados são ingeridos, uma tarefa é executada neles e leva 30 minutos para ser concluída. A carga de trabalho frequentemente apresenta alta latência devido à grande quantidade de dados recebidos. Um arquiteto de soluções precisa projetar uma solução escalável e sem servidor para aprimorar o desempenho.

Qual combinação de etapas o arquiteto de soluções deve adotar? (Selecione duas)

R: Configure o AWS Fargate com o Amazon ECS para processar os dados
R: Configurar o Amazon Kinesis Data Streams para ingerir os dados

Opções corretas:

Configurar o Amazon Kinesis Data Streams para ingerir os dados
Configure o AWS Fargate com o Amazon ECS para processar os dados
O Amazon Kinesis Data Streams (KDS) é um serviço de streaming de dados em tempo real altamente escalável e durável. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes, como fluxos de cliques de sites, fluxos de eventos de bancos de dados, transações financeiras, feeds de mídias sociais, registros de TI e eventos de rastreamento de localização. Os dados coletados ficam disponíveis em milissegundos para permitir casos de uso de análise em tempo real, como painéis em tempo real, detecção de anomalias em tempo real, precificação dinâmica e muito mais.
O AWS Fargate é um mecanismo de computação sem servidor para contêineres que funciona com o Amazon Elastic Container Service (ECS) e o Amazon Elastic Kubernetes Service (EKS). O Fargate facilita o

foco na criação de seus aplicativos. O Fargate elimina a necessidade de provisionar e gerenciar servidores, permite especificar e pagar por recursos por aplicativo e aprimora a segurança por meio do isolamento de aplicativos por design.
Para o caso de uso em questão, podemos usar o Kinesis Data Streams como camada de ingestão e o aplicativo ECS em contêiner no AWS Fargate como camada de processamento. Ambos os componentes são serverless e podem ser escalonados para oferecer o desempenho desejado.

Pergunta 24

A equipe de engenharia de uma empresa de mídia social notou que, embora algumas das imagens armazenadas no Amazon S3 sejam acessadas com frequência, outras ficam ociosas por um período de tempo considerável.
Como arquiteto de soluções, qual é a sua recomendação para criar a solução MAIS econômica?
R: Armazene as imagens usando a classe de armazenamento Amazon S3 Intelligent-Tiering

Opção correta:

Armazene as imagens usando a classe de armazenamento Amazon S3 Intelligent-Tiering
A classe de armazenamento Amazon S3 Intelligent-Tiering foi projetada para otimizar custos, movendo dados automaticamente para a camada de acesso mais econômica, sem impacto no desempenho ou sobrecarga operacional. Ela funciona armazenando objetos em duas camadas de acesso: uma otimizada para acesso frequente e outra de menor custo, otimizada para acesso pouco frequente.
Por uma pequena taxa mensal de monitoramento e automação por objeto, o Amazon S3 monitora os padrões de acesso dos objetos no S3 Intelligent-Tiering e move aqueles que não foram acessados por 30 dias consecutivos para a camada de acesso pouco frequente. Se um objeto na camada de acesso pouco frequente for acessado, ele será automaticamente movido de volta para a camada de acesso frequente. Portanto, usar a classe de armazenamento Amazon S3 Intelligent-Tiering é a solução correta para o problema em questão.

Pergunta 25

A equipe de engenharia de uma empresa de TI está implantando um aplicativo de Processamento Transacional Online (OLTP) que precisa suportar consultas relacionais. O aplicativo terá picos de uso imprevisíveis, dos quais a equipe não tem conhecimento prévio.
Qual banco de dados você recomendaria usar?
R: Amazon Aurora sem servidor

Opção correta:

Amazon Aurora sem servidor
O Amazon Aurora Serverless é uma configuração sob demanda e com escalonamento automático para o Amazon Aurora (edições compatíveis com MySQL e PostgreSQL), onde o banco de dados inicia, encerra e aumenta ou diminui a capacidade automaticamente, de acordo com as necessidades do seu aplicativo. Ele permite que você execute seu banco de dados na nuvem sem precisar gerenciar nenhuma instância. É uma opção simples e econômica para cargas de trabalho pouco frequentes, intermitentes ou imprevisíveis. O design do banco de dados para uma aplicação OLTP se adapta ao modelo relacional, portanto, você pode inferir um sistema OLTP como um Banco de Dados Relacional.
O Amazon Aurora Serverless é a maneira perfeita de criar um banco de dados que pode ser dimensionado para zero servidores e para vários servidores, como um banco de dados OLTP. Portanto, esta é a opção correta.

Pergunta 26

O aplicativo de compras de uma empresa de varejo fica lento quando o tráfego aumenta. O aplicativo possui uma arquitetura de três camadas (web, aplicativo e banco de dados) que utiliza transações síncronas. A equipe de engenharia da empresa identificou alguns gargalos na camada do aplicativo,

mas não deseja alterar a arquitetura do aplicativo subjacente.

Como arquiteto de soluções, qual das seguintes soluções você sugeriria para atender aos tempos de resposta necessários do aplicativo e, ao mesmo tempo, levar em conta quaisquer picos de tráfego?

R: Aproveite o dimensionamento horizontal para as camadas da Web e do aplicativo usando grupos de dimensionamento automático e o balanceador de carga do aplicativo

Opção correta:

Aproveite o dimensionamento horizontal para as camadas da Web e do aplicativo usando grupos de dimensionamento automático e o balanceador de carga do aplicativo

Um sistema horizontalmente escalável é aquele que pode aumentar sua capacidade adicionando mais computadores. Isso contrasta com um sistema verticalmente escalável, que se limita a executar seus processos em apenas um computador; nesses sistemas, a única maneira de aumentar o desempenho é adicionar mais recursos a um computador na forma de CPUs, memória ou armazenamento mais rápidos (ou em maior quantidade).

Sistemas escaláveis horizontalmente muitas vezes conseguem superar sistemas escaláveis verticalmente ao permitir a execução paralela de cargas de trabalho e distribuí-las entre muitos computadores diferentes.

O Elastic Load Balancing é usado para distribuir automaticamente o tráfego de entrada do seu aplicativo entre todas as instâncias do Amazon EC2 em execução. Você pode usar o Elastic Load Balancing para gerenciar as solicitações de entrada, roteando o tráfego de forma otimizada para que nenhuma instância fique sobrecarregada.

Para usar o Elastic Load Balancing com seu grupo de Auto Scaling, você precisa anexar o balanceador de carga ao seu grupo de Auto Scaling para registrá-lo no balanceador de carga. Seu balanceador de carga atua como um único ponto de contato para todo o tráfego da web de entrada no seu grupo de Auto Scaling.

Ao usar o Elastic Load Balancing com seu grupo de Auto Scaling, não é necessário registrar instâncias individuais do Amazon EC2 no balanceador de carga. As instâncias iniciadas pelo seu grupo de Auto Scaling são registradas automaticamente no balanceador de carga. Da mesma forma, as instâncias encerradas pelo seu grupo de Auto Scaling são automaticamente descadastradas do balanceador de carga.

Esta opção exigirá menos alterações de design, mas sim alterações de configuração e a capacidade da camada web/aplicativo de se comunicar entre instâncias. Portanto, esta é a solução ideal para o caso de uso atual.

Pergunta 27

Um aplicativo está hospedado em várias instâncias do Amazon EC2 na mesma Zona de Disponibilidade (AZ). A equipe de engenharia deseja configurar o acesso compartilhado a dados para essas instâncias do Amazon EC2 usando volumes Multi-Attach do Amazon EBS.

Qual tipo de volume do Amazon EBS é a escolha correta para essas instâncias do Amazon EC2?

R: Volumes Amazon EBS de SSD IOPS provisionados

Opção correta:

Volumes Amazon EBS de SSD IOPS provisionados

O Amazon EBS Multi-Attach permite anexar um único volume SSD com IOPS Provisionadas (io1 ou io2) a várias instâncias que estejam na mesma Zona de Disponibilidade. Você pode anexar vários volumes habilitados para Multi-Attach a uma instância ou conjunto de instâncias. Cada instância à qual o volume está anexado tem permissão total de leitura e gravação no volume compartilhado. O Multi-Attach facilita a obtenção de maior disponibilidade de aplicativos em aplicativos Linux em cluster que gerenciam operações de gravação simultâneas.

O Multi-Attach é suportado exclusivamente em volumes SSD IOPS provisionados.

Pergunta 28

A equipe de desenvolvimento de uma empresa gerencia um processo noturno baseado em Python com tempo de execução de 30 minutos. O processo pode suportar qualquer interrupção em sua execução e ser reiniciado. Atualmente, o processo é executado na infraestrutura local e precisa ser migrado para a AWS.

Qual das seguintes opções você recomenda como a solução MAIS econômica?

R: Executar em uma instância Spot com um tipo de solicitação persistente

Opção correta:

Executar em uma instância Spot com um tipo de solicitação persistente

Uma Instância Spot é uma instância não utilizada do Amazon EC2 disponível por um preço menor que o preço sob demanda. Como as Instâncias Spot permitem que você solicite instâncias não utilizadas do Amazon EC2 com grandes descontos, você pode reduzir significativamente seus custos com o Amazon EC2. O preço por hora de uma Instância Spot é chamado de preço Spot. O tipo de solicitação (única ou persistente) determina se a solicitação será aberta novamente quando o Amazon EC2 interromper uma Instância Spot ou se você interromper uma Instância Spot. Se a solicitação for persistente, ela será aberta novamente após a interrupção da sua Instância Spot. Se a solicitação for persistente e você interromper a sua Instância Spot, ela só será aberta após você iniciá-la.

Pergunta 29

Uma empresa possui várias instâncias do Amazon EC2 operando em uma sub-rede privada que faz parte de uma VPC personalizada. Essas instâncias executam um aplicativo de processamento de imagens que precisa acessar imagens armazenadas no Amazon S3. Após o processamento de cada imagem, o status do registro correspondente precisa ser marcado como concluído em uma tabela do Amazon DynamoDB.

Como você forneceria acesso privado a esses recursos da AWS que não fazem parte desta VPC personalizada?

R: Crie um endpoint de gateway separado para Amazon S3 e Amazon DynamoDB cada. Adicione duas novas entradas de destino para esses dois endpoints de gateway na tabela de rotas da VPC personalizada.

Opção correta:

Crie um endpoint de gateway separado para Amazon S3 e Amazon DynamoDB cada. Adicione duas novas entradas de destino para esses dois endpoints de gateway na tabela de rotas da VPC personalizada.

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.

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.

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
Amazon DynamoDB

Pergunta 30

Seu aplicativo de e-commerce utiliza um banco de dados PostgreSQL do Amazon RDS e uma carga de trabalho de análise também é executada no mesmo banco de dados. Quando a carga de trabalho de análise é executada, seu aplicativo de e-commerce fica lento, o que afeta ainda mais suas vendas.

Qual das seguintes opções é a solução MAIS econômica para corrigir esse problema?

R: Crie uma réplica de leitura na mesma região do banco de dados mestre e aponte a carga de trabalho de análise para lá

Opção correta:

Crie uma réplica de leitura na mesma região do banco de dados mestre e aponte a carga de trabalho de análise para lá
As Réplicas de Leitura do Amazon RDS oferecem desempenho e durabilidade aprimorados para instâncias de banco de dados (BD) RDS. Elas facilitam o dimensionamento horizontal elástico, indo além das restrições de capacidade de uma única instância de banco de dados para cargas de trabalho de banco de dados com alto consumo de leitura. Para os mecanismos de banco de dados MySQL, MariaDB, PostgreSQL, Oracle e SQL Server, o Amazon RDS cria uma segunda instância de banco de dados usando um snapshot da instância de banco de dados de origem. Em seguida, ele usa a replicação assíncrona nativa dos mecanismos para atualizar a réplica de leitura sempre que houver uma alteração na instância do banco de dados de origem. As réplicas de leitura podem estar dentro de uma Zona de Disponibilidade, entre AZs ou entre regiões.
Criar uma Réplica de Leitura é a solução. Como queremos minimizar os custos, precisamos iniciar a Réplica de Leitura na mesma região, pois você não será cobrado pela transferência de dados incorrida na replicação entre a instância do banco de dados de origem e a réplica de leitura dentro da mesma região da AWS.
Alerta de exame:
Revise esta comparação entre Multi-AZ e Read Replica para Amazon RDS

Pergunta 31

Uma empresa auxilia seus clientes a assinar legalmente contratos altamente confidenciais. Para atender aos rigorosos requisitos do setor, a empresa precisa garantir que os contratos assinados sejam criptografados usando seu algoritmo proprietário. A empresa está migrando para a Nuvem AWS usando o Amazon Simple Storage Service (Amazon S3) e gostaria que você, o arquiteto de soluções, os aconselhasse sobre o esquema de criptografia a ser adotado.

O que você recomenda?

R: Criptografia do lado do cliente

Opção correta:

Criptografia do lado do cliente
Criptografia do lado do cliente é o ato de criptografar seus dados localmente para ajudar a garantir sua segurança em trânsito e em repouso. Para criptografar seus objetos antes de enviá-los ao Amazon S3, use o Cliente de Criptografia do Amazon S3. Quando seus objetos são criptografados dessa maneira, eles não são expostos a terceiros, incluindo a AWS. O Amazon S3 recebe seus objetos já criptografados; o Amazon S3 não desempenha nenhum papel na criptografia ou descriptografia dos objetos. Você pode usar o Cliente de Criptografia do Amazon S3 e a criptografia do lado do servidor para criptografar seus dados. Quando você envia objetos criptografados ao Amazon S3, o Amazon S3

não os reconhece como criptografados, ele detecta apenas objetos típicos.

Pergunta 32

Uma empresa está transferindo um volume significativo de dados do armazenamento local para a AWS, onde serão acessados por instâncias do Amazon EC2 baseadas em Windows, Mac e Linux na mesma região da AWS, utilizando os protocolos SMB e NFS. Parte desses dados será acessada regularmente, enquanto o restante será acessado com menos frequência. A empresa precisa de uma solução de hospedagem para esses dados que minimize a sobrecarga operacional.

Qual solução atenderia melhor a esses requisitos?

R: Configurar uma instância do Amazon FSx para ONTAP. Configurar um sistema de arquivos FSx para ONTAP no volume raiz e migrar os dados para o volume FSx para ONTAP.

Opção correta:

Configurar uma instância do Amazon FSx para ONTAP. Configurar um sistema de arquivos FSx para ONTAP no volume raiz e migrar os dados para o volume FSx para ONTAP.

O Amazon FSx para NetApp ONTAP é um serviço de armazenamento que permite aos clientes iniciar e executar sistemas de arquivos ONTAP totalmente gerenciados na nuvem. ONTAP é a tecnologia de sistema de arquivos da NetApp que oferece um conjunto amplamente adotado de recursos de acesso e gerenciamento de dados.

O caso de uso apresentado exige que o armazenamento na AWS seja acessado por instâncias do Amazon EC2 baseadas em Windows, Mac e Linux na mesma região da AWS, utilizando os protocolos SMB e NFS. Na família Amazon FSx, o FSx para ONTAP é o único sistema de arquivos que oferece suporte a esse requisito essencial.

Pergunta 33

Uma equipe de desenvolvimento está procurando uma solução que economize tempo de desenvolvimento e custos de implantação para um aplicativo que usa um padrão de mensagem de solicitação-resposta de alto rendimento.

Qual dos seguintes tipos de fila do Amazon SQS é o mais adequado para atender a esse requisito?

R: Filas temporárias do Amazon Simple Queue Service (Amazon SQS)

Opção correta:

Filas temporárias do Amazon Simple Queue Service (Amazon SQS)

Filas temporárias ajudam você a economizar tempo de desenvolvimento e custos de implantação ao usar padrões de mensagens comuns, como solicitação-resposta. Você pode usar o Cliente de Fila Temporária para criar filas temporárias de alto rendimento, econômicas e gerenciadas por aplicativos.

O cliente mapeia automaticamente várias filas temporárias — filas gerenciadas pelo aplicativo, criadas sob demanda para um processo específico — em uma única fila do Amazon SQS. Isso permite que seu aplicativo faça menos chamadas de API e tenha uma taxa de transferência maior quando o tráfego para cada fila temporária estiver baixo. Quando uma fila temporária não estiver mais em uso, o cliente a limpa automaticamente, mesmo que alguns processos que a utilizam não sejam encerrados corretamente.

- A seguir estão os benefícios das filas temporárias:
- Eles servem como canais de comunicação leves para threads ou processos específicos.
- Eles podem ser criados e excluídos sem incorrer em custos adicionais.

- Eles são compatíveis com APIs de filas estáticas (normais) do Amazon SQS. Isso significa que o código existente que envia e recebe mensagens pode enviar e receber mensagens de filas virtuais.

Para oferecer melhor suporte a destinos de mensagens leves e de curta duração, a AWS recomenda o Amazon SQS Temporary Queue Client. Este cliente facilita a criação e a exclusão de diversos destinos de mensagens temporários sem aumentar sua conta da AWS. O conceito-chave por trás do cliente é a fila virtual. As filas virtuais permitem multiplexar muitas filas de baixo tráfego em uma única fila do Amazon SQS. A criação de uma fila virtual apenas instancia um buffer local para armazenar mensagens para os consumidores conforme elas chegam; não há chamada de API para o SQS e não há custos associados à criação de uma fila virtual.

Pergunta 34

Sua empresa criou um data warehouse usando o Amazon Redshift para analisar dados do Amazon S3. A partir do padrão de uso, você detectou que, após 30 dias, os dados raramente são consultados no Amazon Redshift e não são mais "dados importantes". Você gostaria de preservar a capacidade de consulta SQL em seus dados e iniciar as consultas imediatamente. Além disso, você deseja adotar um modelo de preços que permita economizar o máximo possível no Amazon Redshift.

O que você recomenda? (Selecione duas)

R: Mover os dados para o Amazon S3 Standard IA após 30 dias
R: Analise os dados frios com o Amazon Athena

Opções corretas:

Mover os dados para o Amazon S3 Standard IA após 30 dias
O Amazon S3 Standard-IA é para dados acessados com menos frequência, mas que exigem acesso rápido quando necessário. O Amazon S3 Standard-IA oferece alta durabilidade, alta taxa de transferência e baixa latência do S3 Standard, com um preço baixo por GB de armazenamento e uma taxa de recuperação por GB. Essa combinação de baixo custo e alto desempenho torna o S3 Standard-IA ideal para armazenamento de longo prazo, backups e como armazenamento de dados para arquivos de recuperação de desastres. A duração mínima do armazenamento é de 30 dias.

Analise os dados frios com o Amazon Athena
O Amazon Athena é um serviço de consulta interativa que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão. O Athena não requer servidor, portanto, não há infraestrutura para configurar ou gerenciar, e os clientes pagam apenas pelas consultas que executam. Você pode usar o Amazon Athena para processar logs, realizar análises ad-hoc e executar consultas interativas.
Mover os dados para o Amazon S3 Glacier impedirá que possamos consultá-los. Portanto, devemos migrar os dados para o Amazon S3 Standard IA e usar o Amazon Athena para analisar os dados inativos.

Pergunta 35

Uma empresa gerencia um aplicativo de Computação de Alto Desempenho (HPC) que precisa ser implantado em instâncias do Amazon EC2. O aplicativo requer altos níveis de comunicação entre nós e alto tráfego de rede entre as instâncias.

Como arquiteto de soluções, qual das seguintes opções você recomendaria à equipe de engenharia da empresa? (Selecione duas)

R: Implantar instâncias do Amazon EC2 com o Elastic Fabric Adapter (EFA)
R: Implantar instâncias do Amazon EC2 em um grupo de posicionamento de cluster

Opções corretas:

Implantar instâncias do Amazon EC2 com o Elastic Fabric Adapter (EFA)
O Elastic Fabric Adapter (EFA) é uma interface de rede para instâncias do Amazon EC2 que permite aos clientes executar aplicações que exigem altos níveis de comunicação entre nós em escala na AWS.

Sua interface de hardware de bypass do sistema operacional (SO) personalizada aprimora o desempenho das comunicações entre instâncias, o que é essencial para o dimensionamento dessas aplicações. Portanto, esta opção está correta.

Implantar instâncias do Amazon EC2 em um grupo de posicionamento de cluster
Grupos de posicionamento de cluster agrupam instâncias próximas umas das outras dentro de uma Zona de Disponibilidade. Eles são recomendados quando a maior parte do tráfego de rede ocorre entre as instâncias do grupo. Também são recomendados para aplicativos que se beneficiam de baixa latência de rede, alta taxa de transferência de rede ou ambos. Portanto, esta opção é uma das respostas corretas.

Pergunta 36

Uma equipe de engenharia deseja orquestrar vários tipos de tarefas do Amazon ECS em execução em instâncias do Amazon EC2 que fazem parte do cluster do Amazon ECS. Os dados de saída e de estado de todas as tarefas precisam ser armazenados. A quantidade de dados gerada por cada tarefa é de aproximadamente 20 megabytes, e pode haver centenas de tarefas em execução simultaneamente. Como as saídas antigas são arquivadas, espera-se que o tamanho do armazenamento não exceda 1 terabyte.
Como arquiteto de soluções, qual das seguintes opções você recomendaria como solução otimizada para leitura e gravação de alta frequência?
R: Use o Amazon EFS com o modo de throughput provisionado

Opção correta:

Os sistemas de arquivos do Amazon EFS são distribuídos por um número ilimitado de servidores de armazenamento. Esse design de armazenamento de dados distribuído permite que os sistemas de arquivos cresçam elasticamente até a escala de petabytes. Ele também permite acesso paralelo massivo de instâncias de computação, incluindo Amazon EC2, Amazon ECS e AWS Lambda, aos seus dados.

Use o Amazon EFS com o modo de throughput provisionado

O modo Provisioned Throughput está disponível para aplicações com altas taxas de throughput para armazenamento (MiB/s por TiB) ou com requisitos maiores do que os permitidos pelo modo Bursting Throughput. Por exemplo, digamos que você esteja usando o Amazon EFS para ferramentas de desenvolvimento, servidores web ou aplicações de gerenciamento de conteúdo em que a quantidade de dados no seu sistema de arquivos é baixa em relação às demandas de throughput. Seu sistema de arquivos agora pode obter os altos níveis de throughput que seus aplicativos exigem sem precisar sobrecarregá-lo.
Se o seu sistema de arquivos estiver no modo Provisioned Throughput, você poderá aumentá-lo quantas vezes quiser. Você pode diminuir o throughput do seu sistema de arquivos no modo Provisioned Throughput, desde que tenham se passado mais de 24 horas desde a última redução. Além disso, você pode alternar entre o modo Provisioned Throughput e o modo padrão Bursting Throughput, desde que tenham se passado mais de 24 horas desde a última alteração no modo throughput.

Pergunta 37

A equipe de engenharia de uma startup está avaliando o tipo de volume de armazenamento em bloco mais adequado para as instâncias do Amazon EC2 que hospedam seu aplicativo principal. O volume de armazenamento deve suportar latência muito baixa, mas não precisa persistir os dados quando a instância é encerrada. Como arquiteto de soluções, você propôs o uso de volumes de armazenamento de instâncias para atender a esses requisitos.
Quais das seguintes opções você identificaria como as principais características dos volumes do Instance Store? (Selecione duas)
R: Se você criar uma Amazon Machine Image (AMI) a partir de uma instância, os dados em seus volumes de armazenamento de instância não serão preservados

R: Não é possível desanexar um volume de armazenamento de instância de uma instância e anexá-lo a uma instância diferente

Opções corretas:

Não é possível desanexar um volume de armazenamento de instância de uma instância e anexá-lo a uma instância diferente
Você pode especificar volumes de armazenamento de instância para uma instância somente ao iniciá-la. Não é possível desanexar um volume de armazenamento de instância de uma instância e anexá-lo a outra. Os dados em um armazenamento de instância persistem apenas durante o tempo de vida da instância associada. Se uma instância for reinicializada (intencionalmente ou não), os dados no armazenamento de instância persistem.

Se você criar uma Amazon Machine Image (AMI) a partir de uma instância, os dados em seus volumes de armazenamento de instância não serão preservados
Se você criar uma AMI a partir de uma instância, os dados nos volumes de armazenamento de instâncias não serão preservados e não estarão presentes nos volumes de armazenamento de instâncias das instâncias que você iniciar a partir da AMI.

Pergunta 38

Uma empresa de streaming de mídia digital deseja usar o Amazon CloudFront para distribuir seu conteúdo apenas aos assinantes do serviço. Como arquiteto de soluções, qual das seguintes soluções você sugeriria para entregar conteúdo restrito aos usuários finais legítimos? (Selecione duas)
R: Use URLs assinadas do Amazon CloudFront
R: Usar cookies assinados pelo Amazon CloudFront

Opções corretas:

Use URLs assinadas do Amazon CloudFront
Muitas empresas que distribuem conteúdo pela internet querem restringir o acesso a documentos, dados comerciais, fluxos de mídia ou conteúdo destinado a usuários selecionados, por exemplo, usuários que pagaram uma taxa.
Para servir com segurança esse conteúdo privado usando o Amazon CloudFront, você pode fazer o seguinte:
Exija que seus usuários acessem seu conteúdo privado usando URLs assinadas especiais do Amazon CloudFront ou cookies assinados.
Uma URL assinada inclui informações adicionais, como data e hora de validade, que lhe dão mais controle sobre o acesso ao seu conteúdo. Portanto, esta é a opção correta.

Usar cookies assinados pelo Amazon CloudFront
Os cookies assinados do Amazon CloudFront permitem que você controle quem pode acessar seu conteúdo quando você não deseja alterar seus URLs atuais ou quando deseja fornecer acesso a vários arquivos restritos, por exemplo, todos os arquivos na área de assinantes de um site. Portanto, esta também é uma opção correta.

Pergunta 39

Você implantou uma tecnologia de banco de dados com modo de replicação síncrona para sobreviver a desastres em data centers. Portanto, o banco de dados está implantado em duas instâncias do Amazon EC2 em duas Zonas de Disponibilidade (AZs). O banco de dados precisa estar disponível publicamente, portanto, você implantou as instâncias do Amazon EC2 em sub-redes públicas. O protocolo de replicação atualmente usa os endereços IP públicos do Amazon EC2.
O que você pode fazer para diminuir o custo de replicação?
R: Use o IP privado das instâncias do Amazon EC2 para a replicação

Opção correta:

Use o IP privado das instâncias do Amazon EC2 para a replicação
A origem do custo é que o tráfego entre duas instâncias do EC2 passa pela internet pública, gerando altos custos. Nesse caso, a resposta correta é usar um IP privado, para que a rede permaneça privada, por um custo mínimo.

Pergunta 40

Sua aplicação está implantada em instâncias do Amazon EC2, com um Application Load Balancer como front-end. Recentemente, sua infraestrutura foi atacada. Os invasores realizam mais de 100 solicitações por segundo, enquanto seus usuários comuns fazem apenas cerca de 5 solicitações por segundo.
Como você pode evitar eficientemente que invasores sobrecarreguem seu aplicativo?
R: Use um AWS Web Application Firewall (AWS WAF) e configure uma regra baseada em taxa

Opção correta:

Use um AWS Web Application Firewall (AWS WAF) e configure uma regra baseada em taxa
O AWS Web Application Firewall (AWS WAF) é um firewall para aplicações web que ajuda a proteger suas aplicações web ou APIs contra explorações comuns que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. O AWS WAF permite que você controle como o tráfego chega às suas aplicações, permitindo que você crie regras de segurança que bloqueiam padrões de ataque comuns, como injeção de SQL ou script entre sites, e regras que filtram padrões de tráfego específicos que você definir.
A resposta correta é usar WAF (que tem integração com seu ALB) e definir uma regra baseada em taxa.

Pergunta 41

A equipe de engenharia de dados de uma empresa deseja analisar os padrões de acesso ao armazenamento do Amazon S3 para decidir quando transferir os dados certos para a classe de armazenamento correta.
Qual das seguintes opções representa uma opção correta em relação aos recursos de análise de classe de armazenamento do Amazon S3 Analytics?
A análise de classe de armazenamento fornece recomendações apenas para classes IA padrão para padrão

Opção correta:

A análise de classe de armazenamento fornece recomendações apenas para classes IA padrão para padrão
Usando a Análise de Classe de Armazenamento do Amazon S3, você pode analisar padrões de acesso ao armazenamento para ajudar a decidir quando migrar os dados certos para a classe de armazenamento correta. Este novo recurso de análise do Amazon S3 observa padrões de acesso aos dados para ajudar a determinar quando migrar o armazenamento STANDARD, acessado com menos frequência, para a classe de armazenamento STANDARD_IA (IA, para acesso infrequente).
A análise de classe de armazenamento fornece recomendações apenas para classes IA Padrão para Padrão.
Após a análise de classe de armazenamento observar os padrões de acesso pouco frequentes de um conjunto filtrado de dados ao longo de um período, você pode usar os resultados da análise para ajudar a aprimorar suas configurações de ciclo de vida. Você pode configurar a análise de classe de armazenamento para analisar todos os objetos em um bucket. Ou você pode configurar filtros para agrupar objetos para análise por prefixo comum (ou seja, objetos cujos nomes começam com uma string

comum), por tags de objeto ou por prefixo e tags.

Pergunta 42

Uma empresa de compartilhamento de fotos está armazenando fotos de perfil de usuário em um bucket do Amazon S3 e um aplicativo de análise de imagens está implantado em quatro instâncias do Amazon EC2. Um arquiteto de soluções gostaria de acionar um procedimento de análise de imagens em apenas uma das quatro instâncias do Amazon EC2 para cada foto carregada.

O que você recomenda?

R: Crie uma Notificação de Evento do Amazon S3 que envie uma mensagem para uma fila do Amazon SQS. Faça com que as instâncias do Amazon EC2 leiam da fila do Amazon SQS.

Opção correta:

Crie uma Notificação de Evento do Amazon S3 que envie uma mensagem para uma fila do Amazon SQS. Faça com que as instâncias do Amazon EC2 leiam da fila do Amazon SQS.

O recurso de notificação de eventos do Amazon S3 permite que você receba notificações quando determinados eventos ocorrerem no seu bucket. Para habilitar as notificações, você precisa primeiro adicionar uma configuração de notificação que identifique os eventos que você deseja que o Amazon S3 publique e os destinos para onde você deseja que o Amazon S3 envie as notificações.

O Amazon S3 oferece suporte aos seguintes destinos onde pode publicar eventos:

Tópico do Amazon Simple Notification Service (Amazon SNS)

Fila do Amazon Simple Queue Service (Amazon SQS)

AWS Lambda

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

Aqui, precisamos usar as Notificações de Eventos do Amazon S3 (que podem enviar uma mensagem para AWS Lambda, Amazon SNS ou Amazon SQS) para enviar uma mensagem para a fila do Amazon SQS. Ao usar o Amazon SQS, sabemos que apenas uma instância do Amazon EC2 entre as quatro receberá uma mensagem e a processará.

Pergunta 43

Um site de e-commerce está migrando para uma abordagem baseada em microsserviços e planeja expô-lo a partir do mesmo balanceador de carga, vinculado a diferentes grupos-alvo com URLs distintas: checkout.mycorp.com, www.mycorp.com, mycorp.com/products e mycorp.com/orders. O site gostaria de usar o Amazon ECS no backend para gerenciar esses microsserviços e, possivelmente, hospedar o mesmo contêiner da aplicação várias vezes na mesma instância do Amazon EC2.

Qual recurso pode ajudar você a conseguir isso com o mínimo de esforço?

R: Balanceador de carga de aplicativo + mapeamento dinâmico de portas

Opção correta:

Balanceador de carga de aplicativo + mapeamento dinâmico de portas

O Application Load Balancer pode distribuir automaticamente o tráfego de entrada de aplicativos entre vários destinos, como instâncias do Amazon EC2, contêineres, endereços IP e funções do AWS Lambda. Ele pode lidar com a carga variável do tráfego do seu aplicativo em uma única Zona de Disponibilidade ou em várias Zonas de Disponibilidade (AZs).

O mapeamento dinâmico de portas com um Application Load Balancer facilita a execução de várias tarefas no mesmo serviço do Amazon ECS em um cluster do Amazon ECS.

Pergunta 44

A equipe de engenharia de uma empresa de e-commerce deseja configurar um domínio personalizado para uso interno, como internaldomainexample.com. A equipe deseja usar o recurso de zonas privadas hospedadas do Amazon Route 53 para isso.

Quais das seguintes configurações da VPC precisam ser habilitadas? (Selecione duas)

R: enableDnsHostnames
R: habilitar suporte a DNS

Opções corretas:

enableDnsHostnames
habilitar suporte a DNS

Uma zona hospedada privada é um contêiner para registros de um domínio que você hospeda em uma ou mais nuvens privadas virtuais (VPCs) da Amazon. Você cria uma zona hospedada para um domínio (como example.com) e, em seguida, cria registros para informar ao Amazon Route 53 como deseja que o tráfego seja roteado para esse domínio dentro e entre suas VPCs.

Para cada VPC que você deseja associar à zona hospedada do Route 53, altere as seguintes configurações de VPC para verdadeiro:

enableDnsHostnames

habilitar suporte a DNS

Pergunta 45

O CTO de um marketplace online de aluguel de imóveis deseja reprojetar a camada de cache da arquitetura atual para seu banco de dados relacional. O CTO deseja que a camada de cache tenha replicação e suporte a arquivamento integrados à arquitetura.

Qual dos seguintes serviços da AWS oferece os recursos necessários para a reengenharia da camada de cache?

R: Amazon ElastiCache para Redis

Opção correta:

Amazon ElastiCache para Redis

O Amazon ElastiCache para Redis é um armazenamento de dados em memória extremamente rápido que oferece latência abaixo de um milissegundo para alimentar aplicações em tempo real em escala de internet. O Amazon ElastiCache para Redis é uma ótima opção para casos de uso de processamento transacional e analítico em tempo real, como cache, chat/mensagens, tabelas de classificação de jogos, geoespacial, aprendizado de máquina, streaming de mídia, filas, análises em tempo real e armazenamento de sessão. O ElastiCache para Redis oferece suporte imediato à replicação e a snapshots de arquivamento. Portanto, esta é a opção correta.

O Amazon DocumentDB é um serviço de banco de dados de documentos rápido, escalável, altamente disponível e totalmente gerenciado, compatível com cargas de trabalho do MongoDB. Como um banco de dados de documentos, o Amazon DocumentDB facilita o armazenamento, a consulta e a indexação de dados JSON. O DocumentDB não pode ser usado como camada de cache para um banco de dados relacional.

Pergunta 46

Um estúdio de produção de Hollywood está planejando transferir seus ativos de mídia digital existentes, de cerca de 20 petabytes, para a Nuvem AWS no menor prazo possível.

Qual das seguintes opções é uma solução ideal para esse requisito, considerando que os data centers do estúdio estão localizados em um local remoto?

R: AWS Snowmobile

Opção correta:

AWS Snowmobile

O AWS Snowmobile é um serviço de transferência de dados em escala de exabytes usado para mover grandes quantidades de dados para a AWS. Você pode transferir até 100 PB por Snowmobile, um contêiner de transporte robusto de 45 pés de comprimento, puxado por um caminhão semirreboque. O Snowmobile facilita a movimentação de grandes volumes de dados para a nuvem, incluindo bibliotecas de vídeo, repositórios de imagens ou até mesmo uma migração completa de data center. Transferir dados com o Snowmobile é mais seguro, rápido e econômico. A AWS recomenda o uso do Snowmobile para migrar grandes conjuntos de dados de 10 PB ou mais em um único local. Para conjuntos de dados com menos de 10 PB ou distribuídos em vários locais, você deve usar o Snowball.

Pergunta 47

Para suportar cargas de trabalho de produção críticas que exigem resiliência máxima, uma empresa deseja configurar conexões de rede entre sua Amazon VPC e a infraestrutura local. A empresa precisa de conexões AWS Direct Connect com velocidades superiores a 1 Gbps.

Como arquiteto de soluções, qual das seguintes opções você sugeriria como a melhor arquitetura para esse requisito?

R: Opte por duas conexões separadas do AWS Direct Connect terminando em dispositivos separados em mais de um local do Direct Connect

Opção correta:

Opte por duas conexões separadas do AWS Direct Connect terminando em dispositivos separados em mais de um local do Direct Connect

A resiliência máxima é alcançada por conexões separadas que terminam em dispositivos distintos em mais de um local. Essa configuração oferece aos clientes a máxima resiliência a falhas. Como mostrado na figura acima, essa topologia oferece resiliência a falhas de dispositivo, falhas de conectividade e falhas de localização completas. Você pode usar o Direct Connect Gateway para acessar qualquer região da AWS (exceto regiões da AWS na China) de qualquer local do AWS Direct Connect.

Pergunta 48

Uma empresa moveu seus dados críticos de negócios para o Amazon Elastic File System (Amazon EFS), que será acessado por várias instâncias do Amazon EC2.

Como Arquiteto de Soluções Certificado pela AWS - Associado, qual das seguintes opções você recomendaria para exercer o controle de acesso de forma que somente as instâncias permitidas do Amazon EC2 possam ler o sistema de arquivos do Amazon EFS? (Selecione duas)

R: Use uma política do IAM para controlar o acesso de clientes que podem montar seu sistema de arquivos com as permissões necessárias
R: Use grupos de segurança VPC para controlar o tráfego de rede de e para seu sistema de arquivos

Opções corretas:

Use grupos de segurança VPC para controlar o tráfego de rede de e para seu sistema de arquivos

Use uma política do IAM para controlar o acesso de clientes que podem montar seu sistema de arquivos com as permissões necessárias

Você controla quais instâncias do Amazon EC2 podem acessar seu sistema de arquivos Amazon EFS usando regras de grupo de segurança de VPC e políticas do AWS Identity and Access Management (IAM). Use grupos de segurança de VPC para controlar o tráfego de rede de e para seu sistema de arquivos. Anexe uma política do IAM ao seu sistema de arquivos para controlar quais clientes podem montá-lo e com quais permissões. Você também pode usar pontos de acesso do Amazon EFS para gerenciar o acesso a aplicativos. Controle o acesso a arquivos e diretórios com permissões de usuário e grupo compatíveis com POSIX.

Arquivos e diretórios em um sistema de arquivos Amazon EFS oferecem suporte a permissões de leitura, gravação e execução no estilo Unix padrão com base no ID do usuário e nos IDs de grupo. Quando um cliente NFS monta um sistema de arquivos Amazon EFS sem usar um ponto de acesso, o ID do usuário e o ID do grupo fornecidos pelo cliente são considerados confiáveis. Você também pode usar pontos de acesso do Amazon EFS para substituir os IDs de usuário e de grupo usados pelo cliente NFS. Quando os usuários tentam acessar arquivos e diretórios, o Amazon EFS verifica seus IDs de usuário e de grupo para verificar se cada usuário tem permissão para acessar os objetos.

Pergunta 49

Uma equipe de administração de sistemas tem o requisito de executar determinados scripts personalizados apenas uma vez durante o lançamento das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que hospedam seu aplicativo.

Qual das opções a seguir representa a melhor maneira de configurar uma solução para esse requisito com o mínimo de esforço?

R: Execute os scripts personalizados como scripts de dados do usuário nas instâncias do Amazon EC2

Opção correta:

Execute os scripts personalizados como scripts de dados do usuário nas instâncias do Amazon EC2

Ao iniciar uma instância no Amazon EC2, você tem a opção de passar dados do usuário para a instância, que podem ser usados para executar tarefas comuns de configuração automatizada e atémesmo executar scripts após a inicialização da instância. Você pode passar dois tipos de dados do usuário para o Amazon EC2: scripts de shell e diretivas cloud-init.

Por padrão, os scripts de dados do usuário e as diretivas cloud-init são executados apenas durante o ciclo de inicialização, quando você inicia uma instância pela primeira vez. Portanto, nenhuma configuração adicional é necessária, além de incluir os scripts personalizados nos scripts de dados do usuário.

Pergunta 50

A equipe de DevOps de uma grande empresa de serviços financeiros utiliza a implantação de Zonas de Disponibilidade Múltipla (Multi-AZ) para seu banco de dados MySQL Amazon RDS a fim de automatizar a replicação do banco de dados e aumentar a durabilidade dos dados. A equipe de DevOps agendou uma janela de manutenção para uma atualização do mecanismo de banco de dados para o próximo fim de semana.

Qual das seguintes opções é o resultado correto durante a janela de manutenção?

R: Qualquer atualização no nível do mecanismo de banco de dados para uma instância de banco de dados Amazon RDS com implantação Multi-AZ aciona a atualização simultânea das instâncias de banco de dados principal e standby. Isso causa tempo de inatividade até a conclusão da atualização.

Opção correta:

Qualquer atualização no nível do mecanismo de banco de dados para uma instância de banco de dados Amazon RDS com implantação Multi-AZ aciona a atualização simultânea das instâncias de banco de dados principal e standby. Isso causa tempo de inatividade até a conclusão da atualização.

- O Amazon Relational Database Service (Amazon RDS) facilita a configuração, a operação e o escalonamento de um banco de dados relacional na nuvem. Ele oferece capacidade redimensionável e econômica, ao mesmo tempo em que automatiza tarefas administrativas demoradas, como provisionamento de hardware, configuração de banco de dados, aplicação de patches e backups.

Atualizações no nível do mecanismo de banco de dados exigem tempo de inatividade. Mesmo que sua instância de banco de dados do Amazon RDS use uma implantação Multi-AZ, as instâncias de banco de

dados primária e de espera são atualizadas simultaneamente. Isso causa tempo de inatividade até que a atualização seja concluída, e a duração do tempo de inatividade varia de acordo com o tamanho da sua instância de banco de dados.

Pergunta 51

Uma empresa notou diversas exceções de throughput provisionado em seu banco de dados Amazon DynamoDB devido a picos significativos nas gravações no banco de dados. A equipe de desenvolvimento deseja desacoplar a camada de aplicação da camada de banco de dados e dedicar um processo de trabalho para gravar os dados no Amazon DynamoDB.

Qual middleware você recomenda que possa ser escalado infinitamente e atenda a esses requisitos da maneira mais econômica?

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

Opção correta:

Serviço de fila simples da Amazon (Amazon SQS)

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

Usar o Amazon SQS como um middleware nos ajudará a manter a taxa de transferência de gravação durante picos de gravação e, portanto, essa opção é a mais adequada para o caso de uso fornecido.

Pergunta 52

O administrador de sistemas de uma empresa deseja configurar uma arquitetura de alta disponibilidade para uma solução de host bastião.

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

R: Crie um balanceador de carga de rede público que se vincule a instâncias do Amazon EC2 que são hosts bastiões gerenciados por um grupo de dimensionamento automático.

Opção correta:

Crie um balanceador de carga de rede público que se vincule a instâncias do Amazon EC2 que são hosts bastiões gerenciados por 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.

Incluir hosts bastion no seu ambiente VPC permite que você se conecte com segurança às suas instâncias Linux sem expor seu ambiente à internet. Após configurar seus hosts bastion, você poderá acessar as outras instâncias na sua VPC por meio de conexões Secure Shell (SSH) no Linux. Os hosts bastion também são configurados com grupos de segurança para fornecer um controle de entrada preciso.

Você precisa lembrar que os Bastion Hosts usam o protocolo SSH, que é um protocolo baseado em TCP na porta 22. Eles devem ser acessíveis publicamente.

Aqui, a resposta correta é usar um balanceador de carga de rede, que suporta tráfego TCP e permitirá que você se conecte automaticamente à instância do Amazon EC2 no backend.

Pergunta 53

A equipe de engenharia de uma empresa de varejo está planejando migrar do data center local para a Nuvem AWS. A equipe está avaliando o Amazon Relational Database Service (Amazon RDS) como a camada de banco de dados para seu aplicativo principal. A equipe contratou você como Arquiteto de Soluções Associado Certificado pela AWS para assessorá-lo sobre os recursos Multi-AZ do Amazon RDS.

Qual das seguintes opções você identificaria como correta para o Amazon RDS Multi-AZ? (Selecione duas)

R: O Amazon RDS aplica atualizações do sistema operacional executando manutenção no modo de espera, promovendo o modo de espera para primário e, finalmente, executando manutenção no antigo primário, que se torna o novo modo de espera.

R: O Amazon RDS inicia automaticamente um failover para o standby, caso o banco de dados primário falhe por qualquer motivo

Opções corretas:

O Amazon RDS aplica atualizações do sistema operacional executando manutenção no modo de espera, promovendo o modo de espera para primário e, finalmente, executando manutenção no antigo primário, que se torna o novo modo de espera.

Executar uma instância de banco de dados como uma implantação Multi-AZ pode reduzir ainda mais o impacto de um evento de manutenção porque o Amazon RDS aplica atualizações do sistema operacional seguindo estas etapas:

Realizar manutenção no standby.

Promova o standby para primário.

Execute a manutenção no antigo primário, que se torna o novo standby.

Ao modificar o mecanismo de banco de dados da sua instância de banco de dados em uma implantação Multi-AZ, o Amazon RDS atualiza as instâncias de banco de dados primária e secundária simultaneamente. Nesse caso, o mecanismo de banco de dados de toda a implantação Multi-AZ é desativado durante a atualização.

O Amazon RDS inicia automaticamente um failover para o standby, caso o banco de dados primário falhe por qualquer motivo

Você também se beneficia da disponibilidade aprimorada do banco de dados ao executar sua instância de banco de dados como uma implantação Multi-AZ. Em caso de falha na Zona de Disponibilidade ou na instância de banco de dados, o impacto na sua disponibilidade se limita ao tempo que o failover automático leva para ser concluído.

Outro benefício implícito de executar sua instância de banco de dados como uma implantação Multi-AZ é que o failover da instância de banco de dados é automático e não requer administração. Em um contexto do Amazon RDS, isso significa que você não precisa monitorar eventos da instância de banco de dados e iniciar a recuperação manual da instância de banco de dados em caso de falha da Zona de Disponibilidade ou da instância de banco de dados.

Pergunta 54

A equipe de engenharia de uma empresa deseja criar uma tarefa diária de análise de big data utilizando o Spark para analisar dados de vendas online/offline e de fidelidade do cliente, a fim de criar relatórios personalizados para cada cliente. A tarefa de análise de big data precisa ler os dados do Amazon S3 e enviá-los de volta para o Amazon S3.

Qual tecnologia você recomenda para executar o trabalho de análise de Big Data? (Selecione duas)

R: Amazon EMR
R: Cola AWS

Opções corretas:

Amazon EMR

O Amazon EMR é a plataforma de big data em nuvem líder do setor para processamento de grandes volumes de dados usando ferramentas de código aberto como Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi e Presto. Com o EMR, você pode executar análises em escala de petabytes por menos da metade do custo de soluções locais tradicionais e mais de 3 vezes mais rápido do que o Apache Spark padrão. O EMR é usado para iniciar clusters Hadoop/Spark. Para trabalhos de curta duração, você pode iniciar e encerrar clusters e pagar por segundo pelas instâncias utilizadas. Para cargas de trabalho de longa duração, você pode criar clusters de alta disponibilidade que escalam automaticamente para atender à demanda. O Amazon EMR usa o Hadoop, uma estrutura de código aberto, para distribuir seus dados e processamento em um cluster redimensionável de instâncias do Amazon EC2.

Cola AWS

O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado que facilita a preparação e o carregamento de dados para análise pelos clientes. A tarefa do AWS Glue destina-se ao processamento de dados ETL em lote. As tarefas de ETL do AWS Glue podem usar o Amazon S3, armazenamentos de dados em uma VPC ou armazenamentos de dados JDBC locais como origem. As tarefas do AWS Glue extraem dados, os transformam e carregam os dados resultantes de volta para o S3, armazenamentos de dados em uma VPC ou armazenamentos de dados JDBC locais como destino.

Pergunta 55

Uma empresa mantém os dados críticos de seus clientes em um sistema local, criptografados. Ao longo dos anos, a empresa migrou de uma única chave de criptografia para múltiplas chaves de criptografia, dividindo os dados em blocos lógicos. Com a decisão de mover todos os dados para um bucket do Amazon S3, a empresa agora busca uma técnica para criptografar cada arquivo com uma chave de criptografia diferente, a fim de fornecer segurança máxima aos dados locais migrados.

Como você implementará esse requisito sem adicionar a sobrecarga de dividir os dados em grupos lógicos?

R: Configure um único bucket do Amazon S3 para armazenar todos os dados. Use a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) para criptografar os dados.

Opção correta:

Configure um único bucket do Amazon S3 para armazenar todos os dados. Use a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) para criptografar os dados.

A criptografia do lado do servidor é a criptografia dos dados em seu destino pelo aplicativo ou serviço que os recebe. O Amazon S3 criptografa seus dados no nível do objeto, gravando-os em discos em seus data centers, e os descriptografa para você quando você os acessa. Ao usar a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), cada objeto é criptografado com uma chave exclusiva. Como proteção adicional, ele criptografa a própria chave com uma chave raiz que é rotacionada regularmente.

Observação: o Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. A partir de 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 serão criptografados automaticamente, sem custo adicional e sem impacto no desempenho.

Pergunta 56

Você está usando o AWS Lambda para implementar uma tarefa em lote para um fluxo de trabalho de análise de big data. Com base em tendências históricas, uma tarefa semelhante leva em média 30 minutos para ser executada. A função do AWS Lambda extrai dados do Amazon S3, processa-os e, em seguida, grava os resultados de volta no Amazon S3. Ao implantar sua função do AWS Lambda, você notou um problema em que a função do AWS Lambda falhava abruptamente após 15 minutos de execução.

Como arquiteto de soluções, qual das seguintes opções você identificaria como a causa raiz do problema?

R: A função AWS Lambda está com tempo limite esgotado

Opção correta:

O AWS Lambda permite que você execute código sem provisionar ou gerenciar servidores. Você paga apenas pelo tempo de computação consumido.
Com o AWS Lambda, você pode executar código para praticamente qualquer tipo de aplicação ou serviço de back-end, tudo sem precisar de administração. Basta enviar seu código e o Lambda cuida de tudo o que é necessário para executá-lo e escaloná-lo com alta disponibilidade. Você pode configurar seu código para ser acionado automaticamente a partir de outros serviços da AWS ou chamá-lo diretamente de qualquer aplicativo web ou móvel. As funções do AWS Lambda podem ser configuradas para durar até 15 minutos por execução. Você pode definir o tempo limite para qualquer valor entre 1 segundo e 15 minutos.

A função AWS Lambda está com tempo limite esgotado
As funções do AWS Lambda atingem o tempo limite após 15 minutos e geralmente não são destinadas a trabalhos de longa duração.

Pergunta 57

Uma empresa precisa de um serviço do Active Directory para executar cargas de trabalho com reconhecimento de diretório na Nuvem AWS e também deve oferecer suporte à configuração de um relacionamento de confiança com qualquer Microsoft Active Directory local existente.
Qual serviço de diretório da AWS é mais adequado para esse requisito?

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

Opção correta:

Serviço de diretório da AWS para Microsoft Active Directory (AWS Managed Microsoft AD)
O AWS Directory Service permite executar o Microsoft Active Directory (AD) como um serviço gerenciado. O AWS Directory Service para Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, é baseado no Windows Server 2012 R2. Ao selecionar e iniciar esse tipo de diretório, ele é criado como um par de controladores de domínio altamente disponíveis conectados à sua nuvem privada virtual (VPC).
Com o AWS Managed Microsoft AD, você pode executar cargas de trabalho com reconhecimento de diretório na Nuvem AWS, incluindo o Microsoft SharePoint e aplicativos personalizados baseados em .NET e SQL Server. Você também pode configurar uma relação de confiança entre o AWS Managed Microsoft AD na Nuvem AWS e seu Microsoft Active Directory local existente, fornecendo aos usuários e grupos acesso a recursos em qualquer domínio, usando logon único (SSO).
O AWS Managed Microsoft AD é a melhor opção se você precisa de recursos reais do Active Directory para oferecer suporte a aplicativos da AWS ou cargas de trabalho do Windows, incluindo o Amazon Relational Database Service para Microsoft SQL Server. Também é ideal se você deseja um AD autônomo na Nuvem AWS compatível com o Office 365 ou precisa de um diretório LDAP para oferecer suporte aos seus aplicativos Linux.

Pergunta 58

Uma empresa está desenvolvendo uma aplicação de gerenciamento de documentos na AWS. A aplicação é executada em instâncias do Amazon EC2 em múltiplas Zonas de Disponibilidade (AZs). A empresa exige que o repositório de documentos seja altamente disponível e que os documentos sejam devolvidos imediatamente quando solicitados. A equipe de engenharia configurou a aplicação para usar o Amazon Elastic Block Store (Amazon EBS) para armazenar os documentos, mas a equipe está disposta a considerar outras opções para atender ao requisito de disponibilidade.

Como arquiteto de soluções, qual das seguintes opções você recomendaria?

R: Configure o Amazon EBS como o volume raiz da instância do Amazon EC2 e, em seguida, configure o aplicativo para usar o Amazon S3 como o armazenamento de documentos

Opção correta:

Configure o Amazon EBS como o volume raiz da instância do Amazon EC2 e, em seguida, configure o aplicativo para usar o Amazon S3 como o armazenamento de documentos

Instâncias que usam o Amazon EBS como dispositivo raiz têm automaticamente um volume do Amazon EBS anexado. Ao iniciar uma instância com suporte do Amazon EBS, a AWS cria um volume do Amazon EBS para cada snapshot do Amazon EBS referenciado pela AMI que você usa. Uma instância com suporte do Amazon EBS pode ser interrompida e reiniciada posteriormente sem afetar os dados armazenados nos volumes anexados.

O Amazon S3 fornece acesso a uma infraestrutura de armazenamento de dados confiável, rápida e econômica. Ele foi projetado para facilitar a computação em escala web, permitindo que você armazene e recupere qualquer quantidade de dados, a qualquer momento, do Amazon EC2 ou de qualquer lugar na web. O S3 é altamente disponível e pode ser configurado para funcionar como um repositório de documentos para o caso de uso específico.

Pergunta 59

Você está implantando um aplicativo monolítico crítico que precisa ser implantado em um único servidor web, pois não foi criado para funcionar em modo distribuído. Ainda assim, você precisa garantir que sua configuração possa se recuperar automaticamente da falha de uma Zona de Disponibilidade (AZ).

Qual das seguintes opções deve ser combinada para formar a solução MAIS econômica? (Selecione três)

R: Crie um endereço IP elástico (EIP) e use o script de dados do usuário do Amazon EC2 para anexá-lo

R: Atribuir uma função de instância do Amazon EC2 para executar as chamadas de API necessárias

R: Crie um grupo de dimensionamento automático que abranja 2 Zonas de Disponibilidade, onde min=1, max=1, desired=1

Opções corretas:

Crie um grupo de dimensionamento automático que abranja 2 Zonas de Disponibilidade, onde min=1, max=1, desired=1

O Amazon EC2 Auto Scaling ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga do seu aplicativo. Você cria coleções de instâncias do 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.

Portanto, temos um Grupo de Dimensionamento Automático com desired=1, em duas AZs, de modo que, se uma instância cair, ela será recriada automaticamente em outra AZ. Portanto, esta opção está correta.

Crie um endereço IP elástico (EIP) e use o script de dados do usuário do Amazon EC2 para anexá-lo

- O Application Load Balancer (ALB) opera no nível da solicitação (camada 7), roteando o tráfego para destinos – 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 avançado de solicitações voltado para a entrega de arquiteturas de aplicativos modernas, incluindo microsserviços e aplicativos baseados em contêineres.

Um endereço IP elástico é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Um endereço IP elástico é associado à sua conta AWS. Com um endereço IP elástico, você pode mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na sua

conta.
Agora, entre o ALB e o IP Elástico. Se usarmos um ALB, tudo continuará funcionando, mas teremos que pagar pelo ALB provisionado, que envia tráfego para apenas uma instância do Amazon EC2. Em vez disso, para minimizar custos, precisamos usar um IP Elástico.

Atribuir uma função de instância do Amazon EC2 para executar as chamadas de API necessárias
- Para que esse IP elástico seja anexado à nossa instância do Amazon EC2, precisamos usar um script de dados do usuário do EC2, e nossa instância do Amazon EC2 deve ter as permissões corretas do IAM para executar a chamada de API, portanto, precisamos de uma função de instância do Amazon EC2.

Pergunta 60

Uma empresa de varejo precisa de uma conexão segura entre seu data center local e a Nuvem AWS. Essa conexão não requer alta largura de banda e lidará com um pequeno volume de tráfego. A empresa deseja um tempo de resposta rápido para configurar a conexão.
Qual é a maneira MAIS econômica de estabelecer essa conexão?
R: Configurar uma conexão VPN de site para site da AWS

Opção correta:

Configurar uma conexão VPN de site para site da AWS
Por padrão, instâncias que você inicia em uma Amazon VPC não podem se comunicar com sua própria rede (remota). Você pode habilitar o acesso à sua rede remota a partir da sua VPC criando uma conexão AWS Site-to-Site VPN (VPN Site-to-Site) e configurando o roteamento para passar o tráfego pela conexão. Uma conexão VPN refere-se à conexão entre sua VPC e sua própria rede local.
Uma conexão VPN de site para site da AWS oferece dois túneis VPN entre um gateway privado virtual ou um gateway de trânsito no lado da AWS e um gateway do cliente (que representa um dispositivo VPN) no lado remoto (local).
Um gateway privado virtual (VGW) é o concentrador de VPN no lado da Amazon da conexão VPN Site-to-Site da AWS. Você cria um gateway privado virtual e o conecta à VPC a partir da qual deseja criar a conexão VPN Site-to-Site da AWS.

Pergunta 61

Uma empresa de saúde administra uma frota de instâncias do Amazon EC2 em duas sub-redes privadas (chamadas PR1 e PR2) em duas Zonas de Disponibilidade (AZs) denominadas A1 e A2. As instâncias do Amazon EC2 precisam de acesso à internet para gerenciamento de patches do sistema operacional e manutenção de softwares de terceiros. Para facilitar isso, a equipe de engenharia da empresa deseja configurar dois gateways de Tradução de Endereços de Rede (gateways NAT) em uma configuração de alta disponibilidade.
Qual das seguintes opções você sugeriria?
R: Configure um total de dois gateways NAT. O gateway NAT N1 deve ser configurado na sub-rede pública PU1 na Zona de Disponibilidade A1. O gateway NAT N2 deve ser configurado na sub-rede pública PU2 na Zona de Disponibilidade A2.

Opção correta:

Configure um total de dois gateways NAT. O gateway NAT N1 deve ser configurado na sub-rede pública PU1 na Zona de Disponibilidade A1. O gateway NAT N2 deve ser configurado na sub-rede pública PU2 na Zona de Disponibilidade A2.
Um gateway NAT é um serviço de Tradução de Endereços de Rede (NAT). Você pode usar um gateway NAT para que instâncias em uma sub-rede privada possam se conectar a serviços fora da sua VPC, mas serviços externos não possam iniciar uma conexão com essas instâncias.
Para o caso de uso em questão, as instâncias do Amazon EC2 nas sub-redes privadas podem se conectar à internet por meio de gateways NAT públicos em suas respectivas Zonas de Disponibilidade (AZ). Você deve criar um gateway NAT público na sub-rede pública de cada AZ e associar um endereço IP

elástico ao gateway NAT na criação. Em seguida, você pode rotear o tráfego do gateway NAT para o gateway de internet da VPC.
Se você tiver recursos em várias Zonas de Disponibilidade e elas compartilharem um gateway NAT, e se a Zona de Disponibilidade do gateway NAT estiver inativa, os recursos nas outras Zonas de Disponibilidade perderão o acesso à internet. Para criar uma arquitetura de alta disponibilidade ou independente de Zona de Disponibilidade, crie um gateway NAT em cada Zona de Disponibilidade e configure seu roteamento para garantir que os recursos usem o gateway NAT na mesma Zona de Disponibilidade.

Pergunta 62

Como Arquiteto de Soluções, você gostaria de proteger completamente as comunicações entre sua distribuição do Amazon CloudFront e seu bucket do Amazon S3, que contém os arquivos estáticos do seu site. Os usuários só devem conseguir acessar o bucket do Amazon S3 por meio do Amazon CloudFront e não diretamente.

O que você recomenda?

R: Crie uma identidade de acesso de origem (OAI) e atualize a política de bucket do Amazon S3

Opção correta:

Crie uma identidade de acesso de origem (OAI) e atualize a política de bucket do Amazon S3
Para restringir o acesso ao conteúdo que você fornece dos buckets do Amazon S3, siga as seguintes etapas:

- Crie um usuário especial do Amazon CloudFront chamado identidade de acesso de origem (OAI) e associe-o à sua distribuição.
- Configure as permissões do seu bucket do Amazon S3 para que o Amazon CloudFront possa usar o OAI para acessar os arquivos no seu bucket e disponibilizá-los aos seus usuários. Certifique-se de que os usuários não possam usar uma URL direta para o bucket do Amazon S3 para acessar um arquivo nele.
- Depois de seguir essas etapas, os usuários só poderão acessar seus arquivos por meio do Amazon CloudFront, não diretamente do bucket do Amazon S3.

Em geral, se você estiver usando um bucket do Amazon S3 como origem para uma distribuição do Amazon CloudFront, poderá permitir que todos tenham acesso aos arquivos ou restringir o acesso. Se você restringir o acesso usando, por exemplo, URLs assinadas do Amazon CloudFront ou cookies assinados, também não desejará que as pessoas visualizem os arquivos simplesmente usando a URL direta do Amazon S3 para o arquivo. Em vez disso, você deseja que elas acessem os arquivos apenas usando a URL do Amazon CloudFront, para que seu conteúdo permaneça protegido.

Pergunta 63

Uma empresa de saúde deseja executar seus aplicativos em hardware de locatário único para atender às diretrizes de conformidade.

Qual das seguintes opções é a maneira MAIS econômica de isolar as instâncias do Amazon EC2 para um único locatário?

R: Instâncias dedicadas

Opção correta:

Instâncias dedicadas
Instâncias Dedicadas são instâncias do Amazon EC2 executadas em uma nuvem privada virtual (VPC) em hardware dedicado a um único cliente. Instâncias Dedicadas que pertencem a diferentes contas da AWS são fisicamente isoladas em nível de hardware, mesmo que essas contas estejam vinculadas a uma conta de pagador único. No entanto, Instâncias Dedicadas podem compartilhar hardware com outras instâncias da mesma conta da AWS que não sejam Instâncias Dedicadas.
Um Host Dedicado também é um servidor físico dedicado ao seu uso. Com um Host Dedicado, você tem visibilidade e controle sobre como as instâncias são alocadas no servidor.

Pergunta 64

Um estagiário de engenharia de software em uma empresa está documentando os recursos oferecidos pelas instâncias Spot e frotas Spot do Amazon EC2.

Você pode ajudar o estagiário selecionando as opções corretas que identificam as principais características desses dois tipos de entidades Spot? (Selecione duas)

R: Uma frota Spot pode consistir em um conjunto de instâncias Spot e, opcionalmente, instâncias On-Demand que são lançadas para atender à sua capacidade alvo

R: Instâncias spot são capacidade extra do Amazon EC2 que podem gerar até 90% de desconto em relação aos preços sob demanda. Instâncias spot podem ser interrompidas pelo Amazon EC2 para atender a requisitos de capacidade com uma notificação de 2 minutos.

Opções corretas:

Instâncias spot são capacidade extra do Amazon EC2 que podem gerar até 90% de desconto em relação aos preços sob demanda. Instâncias spot podem ser interrompidas pelo Amazon EC2 para atender a requisitos de capacidade com uma notificação de 2 minutos.

Instâncias Spot são capacidades extras do Amazon EC2 que podem gerar até 90% de desconto em relação aos preços sob demanda, e que a Amazon Web Services pode interromper com uma notificação de 2 minutos. Como as Instâncias Spot permitem que você solicite instâncias do EC2 não utilizadas com grandes descontos, você pode reduzir significativamente seus custos com o Amazon EC2. As Instâncias Spot são uma opção econômica se você puder ser flexível quanto ao horário de execução e à possibilidade de interrupção de seus aplicativos.

Uma frota Spot pode consistir em um conjunto de instâncias Spot e, opcionalmente, instâncias On-Demand que são lançadas para atender à sua capacidade alvo

Uma frota Spot é um conjunto, ou frota, de Instâncias Spot e, opcionalmente, Instâncias On-Demand. A frota Spot tenta iniciar o número de Instâncias Spot e Instâncias On-Demand necessário para atingir a capacidade-alvo especificada na solicitação da frota Spot. Uma frota Spot permite que você solicite e gerencie automaticamente várias instâncias Spot que oferecem o menor preço por unidade de capacidade para seu cluster ou aplicativo, como uma tarefa de processamento em lote, um fluxo de trabalho Hadoop ou uma tarefa de computação em grade HPC.

Pergunta 65

A equipe de engenharia de uma empresa multinacional usa o AWS Firewall Manager para configurar e gerenciar centralmente regras de firewall em suas contas e aplicativos usando o AWS Organizations.

Em quais dos seguintes recursos da AWS o AWS Firewall Manager pode configurar regras? (Selecione três)

R: Firewall de aplicativo da Web da AWS (AWS WAF) R: Grupos de segurança de VPC
R: AWS Shield Avançado

Opções corretas:

Firewall de aplicativo da Web da AWS (AWS WAF) AWS Shield Avançado
Grupos de segurança de VPC

O AWS Firewall Manager é um serviço de gerenciamento de segurança que permite configurar e gerenciar centralmente regras de firewall em suas contas e aplicativos no AWS Organizations. À medida que novos aplicativos são criados, o Firewall Manager facilita a conformidade de novos aplicativos e recursos, aplicando um conjunto comum de regras de

segurança. Agora você tem um único serviço para criar regras de firewall, criar políticas de segurança e aplicá-las de forma consistente e hierárquica em toda a sua infraestrutura.
Com o AWS Firewall Manager, você pode configurar centralmente as regras do AWS WAF, a proteção avançada do AWS Shield, os grupos de segurança da Amazon Virtual Private Cloud (VPC), os firewalls de rede da AWS e as regras do firewall DNS do Amazon Route 53 Resolver em todas as contas e recursos da sua organização. Atualmente, ele não oferece suporte a ACLs de rede.