Pergunta 1

O gerente de engenharia de um aplicativo de gerenciamento de conteúdo quer configurar réplicas de leitura do Amazon RDS para fornecer desempenho aprimorado e escalabilidade de leitura. O gerente quer entender as taxas de transferência de dados ao configurar réplicas de leitura do Amazon RDS.

Qual das seguintes opções você identificaria como correta em relação às taxas de transferência de dados para réplicas de leitura do Amazon RDS?

R: Há taxas de transferência de dados para replicar dados entre regiões da AWS

Opção correta:

Há taxas de transferência de dados para replicar dados entre regiões da AWS

As réplicas de leitura do Amazon RDS fornecem desempenho e durabilidade aprimorados para instâncias de banco de dados (DB) do Amazon RDS. Elas facilitam o dimensionamento elástico além das restrições de capacidade de uma única instância de DB para cargas de trabalho de banco de dados com leitura pesada. Uma réplica de leitura é cobrada como uma Instância de BD padrão e nas mesmas taxas. Você não é cobrado pela transferência de dados incorrida na replicação de dados entre sua instância de BD de origem e a réplica de leitura dentro da mesma Região da AWS.

Pergunta 2

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

Qual das opções a seguir é a maneira MAIS econômica de isolar suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) para um único locatário?

R: Instâncias dedicadas

Opção correta:

Instâncias dedicadas

Instâncias Dedicadas são instâncias do Amazon EC2 que são 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 um nível de hardware, mesmo se essas contas estiverem vinculadas a uma conta de pagador único. No entanto, Instâncias Dedicadas podem compartilhar hardware com outras instâncias da mesma conta da AWS que não são Instâncias Dedicadas.
Um Host Dedicado também é um servidor físico dedicado para seu uso. Com um Host Dedicado, você tem visibilidade e controle sobre como as instâncias são colocadas no servidor.

Pergunta 3

Uma empresa de varejo quer compartilhar dados contábeis confidenciais armazenados em uma instância de banco de dados Amazon RDS com um auditor externo. O auditor tem sua própria conta AWS e precisa de sua própria cópia do banco de dados.

Qual das opções a seguir você recomendaria para compartilhar com segurança o banco de dados com o auditor?

R: Crie um instantâneo criptografado do banco de dados, compartilhe o instantâneo e permita o acesso à chave de criptografia do AWS Key Management Service (AWS KMS)

Opção correta:

Crie um instantâneo criptografado do banco de dados, compartilhe o instantâneo e permita o acesso à chave de criptografia do AWS Key Management Service (AWS KMS)

Você pode compartilhar a chave do AWS Key Management Service (AWS KMS) que foi usada para criptografar o snapshot com qualquer conta que você queira que possa acessar o snapshot. Você pode compartilhar a AWS KMS Key com outra conta da AWS adicionando a outra conta à política de chave do AWS KMS.
Fazer um instantâneo criptografado do banco de dados dará ao auditor uma cópia do banco de dados, conforme necessário para o caso de uso específico.

Pergunta 4

Uma empresa de TI fornece acesso ao bucket do Amazon Simple Storage Service (Amazon S3) para usuários específicos dentro da mesma conta para concluir o trabalho específico do projeto. Com a mudança dos requisitos de negócios, as solicitações de acesso S3 entre contas também estão crescendo a cada mês. A empresa está procurando uma solução que possa oferecer permissões de acesso em nível de usuário e de conta para os dados armazenados nos buckets do Amazon S3.

Como arquiteto de soluções, qual das opções a seguir você sugeriria como a maneira MAIS otimizada de controlar o acesso para esse caso de uso?

R: Usar políticas de bucket do Amazon S3

Opção correta:

Usar políticas de bucket do Amazon S3
As políticas de bucket no Amazon S3 podem ser usadas para adicionar ou negar permissões em alguns ou todos os objetos dentro de um único bucket. As políticas podem ser anexadas a usuários, grupos ou buckets do Amazon S3, permitindo o gerenciamento centralizado de permissões. Com as políticas de bucket, você pode conceder aos usuários dentro da sua conta da AWS ou de outras contas da AWS acesso aos seus recursos do Amazon S3.
Você pode restringir ainda mais o acesso a recursos específicos com base em certas condições. Por exemplo, você pode restringir o acesso com base no horário da solicitação (Date Condition), se a solicitação foi enviada usando SSL (Boolean Conditions), no endereço IP de um solicitante (IP Address Condition) ou com base no aplicativo cliente do solicitante (String Conditions). Para identificar essas condições, você usa chaves de política.

Pergunta 5

Uma empresa de TI criou uma solução na qual um cluster do Amazon Redshift grava dados em um bucket do Amazon S3 pertencente a uma conta diferente da AWS. No entanto, descobriu-se que os arquivos criados no bucket do Amazon S3 usando o comando UNLOAD do cluster do Amazon Redshift nem mesmo são acessíveis ao proprietário do bucket do Amazon S3.

Qual poderia ser o motivo dessa negação de permissão para o proprietário do balde?

R: Por padrão, um objeto Amazon S3 é de propriedade da conta AWS que o carregou. Portanto, o proprietário do bucket Amazon S3 não terá acesso implícito aos objetos gravados pelo cluster Amazon Redshift

Opção correta:

Por padrão, um objeto do Amazon S3 é de propriedade da conta da AWS que o carregou. Portanto, o proprietário do bucket do Amazon S3 não terá acesso implícito aos objetos gravados pelo cluster do Amazon Redshift
- Por padrão, um objeto do Amazon S3 é de propriedade da conta da AWS que o carregou. Isso é verdadeiro mesmo quando o bucket é de propriedade de outra conta. Como os arquivos de dados do Amazon Redshift do comando UNLOAD foram colocados no seu bucket por outra conta, você (o proprietário do bucket) não tem permissão padrão para acessar esses arquivos.
Para obter acesso aos arquivos de dados, uma função do AWS Identity and Access Management (IAM) com permissões entre contas deve executar o comando UNLOAD novamente. Siga estas etapas para configurar o cluster do Amazon Redshift com permissões entre contas para o bucket:

- Na conta do bucket do Amazon S3, crie uma função do IAM (Bucket Role) com permissões para o bucket.
- Na conta do cluster do Amazon Redshift, crie outra função do IAM (função de cluster) com permissões para assumir a função de bucket.
- Atualize a função do bucket para conceder acesso ao bucket e criar um relacionamento de confiança com a função do cluster.
- No cluster do Amazon Redshift, execute o comando UNLOAD usando a função de cluster e a função de bucket.

Esta solução não se aplica a clusters do Amazon Redshift ou buckets do Amazon S3 que usam criptografia do lado do servidor com o AWS Key Management Service (AWS KMS).

Pergunta 6

Um aplicativo executa cargas de trabalho de big data em instâncias do Amazon Elastic Compute Cloud (Amazon EC2). O aplicativo é executado 24x7 durante todo o ano e precisa de pelo menos 20 instâncias para manter um limite mínimo de desempenho aceitável e o aplicativo precisa de 300 instâncias para lidar com picos na carga de trabalho. Com base nas cargas de trabalho históricas processadas pelo aplicativo, ele precisa de 80 instâncias 80% do tempo.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução com melhor custo-benefício para que ela possa atender à demanda de carga de trabalho de forma estável?

R: Compre 80 instâncias reservadas (RIs). Provisione instâncias adicionais sob demanda e spot conforme a demanda da carga de trabalho (Use o Auto Scaling Group com o modelo de inicialização para provisionar a mistura de instâncias sob demanda e spot)

Opção correta:

Compre 80 instâncias reservadas (RIs). Provisione instâncias adicionais sob demanda e spot conforme a demanda da carga de trabalho (Use o Auto Scaling Group com o modelo de inicialização para provisionar a mistura de instâncias sob demanda e spot)

Como a demanda de carga de trabalho em estado estável é de 80 instâncias, podemos economizar em custos comprando 80 instâncias reservadas. Com base na demanda de carga de trabalho adicional, podemos especificar uma mistura de instâncias sob demanda e spot usando o Application Load Balancer com um modelo de inicialização para provisionar a mistura de instâncias sob demanda e spot.

Veja esta visão geral detalhada de vários tipos de instâncias do Amazon EC2 de uma perspectiva de preço:

Pergunta 7

Um aplicativo está atualmente hospedado em quatro instâncias do Amazon EC2 (atrás do Application Load Balancer) implantadas em uma única Availability Zone (AZ). Para manter um nível aceitável de experiência do usuário final, o aplicativo precisa de pelo menos 4 instâncias para estar sempre disponível.

Como arquiteto de soluções, qual das opções a seguir você recomendaria para que o aplicativo atinja alta disponibilidade com custo MÍNIMO?

R: Implante as instâncias em três Zonas de Disponibilidade (AZs). Inicie duas instâncias em cada Zona de Disponibilidade (AZ)

Opção correta:

Implante as instâncias em três Zonas de Disponibilidade (AZs). Inicie duas instâncias em cada Zona de Disponibilidade (AZ)

A opção correta é implantar as instâncias em três Zonas de Disponibilidade (AZs) e iniciar duas instâncias em cada Zona de Disponibilidade (AZ). Mesmo que uma das AZs fique fora de serviço, ainda teremos 4 instâncias disponíveis e o aplicativo pode manter um nível aceitável de experiência do

usuário final. Portanto, podemos atingir alta disponibilidade com apenas 6 instâncias neste caso.

Pergunta 8

Você gostaria de usar o AWS Snowball para mover backups locais para uma camada de arquivamento de longo prazo na AWS. Qual solução fornece a MAIOR economia de custos?
R: Crie um trabalho do AWS Snowball e direcione um bucket do Amazon S3. Crie uma política de ciclo de vida para fazer a transição desses dados para o Amazon S3 Glacier Deep Archive no mesmo dia

Opção correta:

Crie um trabalho do AWS Snowball e direcione um bucket do Amazon S3. Crie uma política de ciclo de vida para fazer a transição desses dados para o Amazon S3 Glacier Deep Archive no mesmo dia
O AWS Snowball, parte da família AWS Snow, é um dispositivo de migração de dados e edge computing que vem em duas opções. Os dispositivos Snowball Edge Storage Optimized fornecem armazenamento em bloco e armazenamento de objetos compatível com Amazon S3 e 40 vCPUs. Eles são adequados para armazenamento local e transferência de dados em larga escala. Os dispositivos AWS Snowball Edge Compute Optimized fornecem 52 vCPUs, armazenamento em bloco e objeto e uma GPU opcional para casos de uso como aprendizado de máquina avançado e análise de vídeo em movimento completo em ambientes desconectados.
O AWS Snowball Edge Storage Optimized é a escolha ideal se você precisa transferir de forma segura e rápida dezenas de terabytes para petabytes de dados para a AWS. Ele fornece até 80 terabytes de armazenamento HDD utilizável, 40 vCPUs, 1 terabyte de armazenamento SATA SSD e até 40 gigabytes de conectividade de rede para lidar com casos de uso de transferência de dados em larga escala e pré-processamento.
Os dispositivos AWS Snowball originais foram retirados de serviço e o AWS Snowball Edge Storage Optimized agora é o dispositivo primário usado para transferência de dados. Você pode ver o dispositivo AWS Snowball no exame, mas lembre-se de que o dispositivo AWS Snowball original tinha 80 terabytes de espaço de armazenamento.
Para este cenário, você vai querer minimizar o tempo gasto no Amazon S3 Standard para todos os arquivos para evitar cobranças não intencionais de armazenamento do Amazon S3 Standard. Para fazer isso, a AWS recomenda usar uma política de ciclo de vida de dia zero. De uma perspectiva de custo, ao usar uma política de ciclo de vida de dia zero, você só é cobrado pelas taxas do Amazon S3 Glacier Deep Archive. Quando faturado, a política de ciclo de vida é contabilizada primeiro e, se o destino for o Amazon S3 Glacier Deep Archive, você é cobrado pelas taxas do Amazon S3 Glacier Deep Archive para os arquivos transferidos.
Você não pode mover dados diretamente do AWS Snowball para o Amazon S3 Glacier, você precisa passar pelo Amazon S3 primeiro e então usar uma política de ciclo de vida. Então essa opção está correta.

Pergunta 9

Uma empresa de análise quer melhorar o desempenho de seus fluxos de trabalho de processamento de big data em execução no Amazon Elastic File System (Amazon EFS). Qual dos seguintes modos de desempenho deve ser usado para o Amazon EFS para atender a esse requisito?
R: Máx. E/S

Opção correta:

Máx. E/S
O modo de desempenho Max I/O é usado para escalar para níveis mais altos de throughput agregado e operações por segundo. Esse dimensionamento é feito com uma troca de latências ligeiramente maiores para operações de metadados de arquivo. Aplicativos e cargas de trabalho altamente paralelizados, como análise de big data, processamento de mídia e análise genômica, podem se beneficiar desse modo.

Pergunta 10

O que esta política de IAM faz?

```
{
  "Version": "2012-10-17",
      "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "eu-west-1"
        }
      }
    }
  ]
  }
```

R: Ele permite executar instâncias do Amazon EC2 apenas na `eu-west-1` região, e a chamada da API pode ser feita de qualquer lugar do mundo

Opção correta:

Ele permite executar instâncias do Amazon EC2 apenas na `eu-west-1` região, e a chamada da API pode ser feita de qualquer lugar do mundo

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

Você pode usar a `aws:RequestedRegion` chave para comparar a Região da AWS que foi chamada na solicitação com a Região que você especificou na política. Você pode usar essa chave de condição global para controlar quais Regiões podem ser solicitadas.

`aws:RequestedRegion` representa o alvo da chamada de API. Então, neste exemplo, podemos apenas iniciar uma instância do Amazon EC2 em `eu-west-1` , e podemos fazer essa chamada de API de qualquer lugar.

Pergunta 11

Uma empresa de TI está trabalhando em um projeto de cliente para criar um aplicativo de Supply Chain Management. A camada da web do aplicativo é executada em uma instância do Amazon EC2 e a camada do banco de dados está no Amazon RDS MySQL. Para testes beta, todos os recursos estão atualmente implantados em uma única Availability Zone (AZ). A equipe de desenvolvimento quer melhorar a disponibilidade do aplicativo antes do go-live.

Considerando que todos os usuários finais do aplicativo web estariam localizados nos EUA, qual das seguintes opções seria a solução MAIS eficiente em termos de recursos?

R: Implante as instâncias do Amazon EC2 da camada da Web em duas Zonas de Disponibilidade (AZs), atrás de um Elastic Load Balancer. Implante o banco de dados MySQL do Amazon RDS na configuração Multi-AZ

Opção correta:

Implante as instâncias do Amazon EC2 da camada da Web em duas Zonas de Disponibilidade (AZs), atrás de um Elastic Load Balancer. Implante o banco de dados MySQL do Amazon RDS na configuração Multi-AZ
O Elastic Load Balancing distribui automaticamente o tráfego de entrada do aplicativo em vários destinos, como instâncias do Amazon EC2, contêineres, endereços IP e funções 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. Portanto, implantar as instâncias do Amazon EC2 da camada da web em duas Zonas de Disponibilidade (AZs), atrás de um Elastic Load Balancer, melhoraria a disponibilidade do aplicativo.
As implantações Multi-AZ do Amazon RDS fornecem disponibilidade e durabilidade aprimoradas para instâncias de banco de dados (DB) do RDS, tornando-as um ajuste natural para cargas de trabalho de banco de dados de produção. Quando você provisiona uma Instância de BD Multi-AZ, o Amazon RDS cria automaticamente uma Instância de BD primária e replica os dados de forma síncrona para uma instância de espera em uma Zona de Disponibilidade (AZ) diferente. Cada Zona de Disponibilidade (AZ) é executada em sua própria infraestrutura fisicamente distinta e independente, e é projetada para ser altamente confiável. A implantação do banco de dados MySQL do Amazon RDS na configuração Multi-AZ melhoraria a disponibilidade e, portanto, esta é a opção correta.

Pergunta 12

Uma empresa de e-commerce opera várias contas AWS e interconectou essas contas em um estilo hub-and-spoke usando o AWS Transit Gateway. A Amazon Virtual Private Cloud (Amazon VPCs) foi provisionada nessas contas AWS para facilitar o isolamento da rede.

Qual das seguintes soluções reduziria tanto a sobrecarga administrativa quanto os custos, ao mesmo tempo em que forneceria acesso compartilhado aos serviços exigidos pelas cargas de trabalho em cada uma das VPCs?

R: Crie uma Amazon Virtual Private Cloud (Amazon VPC) de serviços compartilhados

Opção correta:

Crie uma Amazon Virtual Private Cloud (Amazon VPC) de serviços compartilhados
Considere uma organização que construiu uma rede hub-and-spoke com o AWS Transit Gateway. VPCs foram provisionadas em várias contas da AWS, talvez para facilitar o isolamento da rede ou para permitir a administração de rede delegada. Ao implantar arquiteturas distribuídas como essa, uma abordagem popular é construir uma "VPC de serviços compartilhados", que fornece acesso aos serviços exigidos pelas cargas de trabalho em cada uma das VPCs. Isso pode incluir serviços de diretório ou endpoints de VPC. Compartilhar recursos de um local central em vez de criá-los em cada VPC pode reduzir a sobrecarga e o custo administrativo.

Um endpoint VPC permite que você conecte privadamente seu VPC a serviços AWS suportados sem exigir um gateway de Internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. Endpoints são dispositivos virtuais que são componentes VPC escalonados horizontalmente, redundantes e altamente disponíveis. Eles permitem a comunicação entre instâncias em seu VPC e serviços sem impor riscos de disponibilidade ou restrições de largura de banda em seu tráfego de rede.

Os endpoints de VPC permitem que você reduza as taxas de transferência de dados resultantes da comunicação de rede entre recursos privados de VPC (como instâncias do Amazon Elastic Cloud Compute — ou EC2) e serviços da AWS (como o Amazon Quantum Ledger Database ou QLDB). Sem endpoints de VPC configurados, as comunicações que se originam de dentro de uma VPC destinada a serviços públicos da AWS devem sair da AWS para a Internet pública para acessar os serviços da AWS. Esse caminho de rede

incorre em taxas de transferência de dados de saída. As taxas de transferência de dados para tráfego que sai do Amazon EC2 para a Internet variam com base no volume. Com endpoints de VPC configurados, a comunicação entre sua VPC e o serviço AWS associado não sai da rede da Amazon. Se sua carga de trabalho exigir que você transfira volumes significativos de dados entre sua VPC e a AWS, você pode reduzir custos aproveitando endpoints de VPC.

Pergunta 13

A equipe de engenharia de uma empresa de logística percebeu que o grupo de dimensionamento automático (ASG) não está encerrando uma instância do Amazon EC2 com problemas.

Como arquiteto de soluções, qual das seguintes opções você sugeriria para solucionar o problema?

(Selecione três)

Uma verificação de integridade personalizada pode ter falhado. O grupo de dimensionamento automático (ASG) não encerra instâncias que são definidas como não íntegras por verificações personalizadas

Sua seleção está correta

R: A instância pode estar em status prejudicado
R: O período de carência da verificação de integridade da instância não expirou
R: A instância falhou na verificação de status de integridade do Elastic Load Balancing (ELB)

Opções corretas:

O período de carência da verificação de integridade da instância não expirou

O Amazon EC2 Auto Scaling não encerra uma instância que entrou em serviço com base nas verificações de status do Amazon EC2 e nas verificações de integridade do Elastic Load Balancing (ELB) até que o período de carência da verificação de integridade expire.

A instância pode estar em status prejudicado
O Amazon EC2 Auto Scaling não encerra imediatamente instâncias com status Impaired. Em vez disso, o Amazon EC2 Auto Scaling aguarda alguns minutos para que a instância se recupere. O Amazon EC2 Auto Scaling também pode atrasar ou não encerrar instâncias que não relatam dados para verificações de status. Isso geralmente acontece quando não há dados suficientes para as métricas de verificação de status no Amazon CloudWatch.

A instância falhou na verificação de status de integridade do Elastic Load Balancing (ELB)
Por padrão, o Amazon EC2 Auto Scaling não usa os resultados das verificações de integridade do ELB para determinar o status de integridade de uma instância quando a configuração de verificação de integridade do grupo está definida como EC2. Como resultado, o Amazon EC2 Auto Scaling não encerra instâncias que falham nas verificações de integridade do ELB. Se o status de uma instância for OutofService no console do ELB, mas o status da instância for Healthy no console do Amazon EC2 Auto Scaling, confirme se o tipo de verificação de integridade está definido como ELB.

Pergunta 14

Uma empresa tem muitas Amazon Virtual Private Cloud (Amazon VPC) em várias contas, que precisam ser conectadas em uma rede estrela entre si e conectadas com redes locais por meio do AWS Direct Connect.

O que você recomenda?

R: Gateway de trânsito da AWS

Opção correta:

Gateway de trânsito da AWS
O AWS Transit Gateway é um serviço que permite que os clientes conectem suas Amazon Virtual Private Clouds (VPCs) e suas redes locais a um único gateway. Com o AWS Transit Gateway, você só precisa criar

e gerenciar uma única conexão do gateway central para cada Amazon VPC, data center local ou escritório remoto em sua rede. O Transit Gateway atua como um hub que controla como o tráfego é roteado entre todas as redes conectadas que agem como spokes. Portanto, este é um caso de uso perfeito para o Transit Gateway.

Pergunta 15

Uma empresa lançou recentemente um novo aplicativo de jogos para dispositivos móveis que os usuários estão adotando rapidamente. A empresa usa o Amazon RDS MySQL como banco de dados. A equipe de engenharia quer uma solução urgente para esse problema em que a carga de trabalho em rápido crescimento pode exceder o armazenamento de banco de dados disponível.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria para que fosse necessário o mínimo de esforço de desenvolvimento e administração de sistemas para atender a esse requisito?

R: Habilitar dimensionamento automático de armazenamento para Amazon RDS MySQL

Opção correta:

Habilitar dimensionamento automático de armazenamento para Amazon RDS MySQL

Se sua carga de trabalho for imprevisível, você pode habilitar o dimensionamento automático de armazenamento para uma instância de banco de dados do Amazon RDS. Com o dimensionamento automático de armazenamento habilitado, quando o Amazon RDS detecta que você está ficando sem espaço livre no banco de dados, ele dimensiona automaticamente seu armazenamento. O Amazon RDS inicia uma modificação de armazenamento para uma instância de banco de dados habilitada para dimensionamento automático quando estes fatores se aplicam:

O espaço livre disponível é inferior a 10% do armazenamento alocado.

A condição de armazenamento baixo dura pelo menos cinco minutos.

Pelo menos seis horas se passaram desde a última modificação de armazenamento.

O limite máximo de armazenamento é o limite que você define para dimensionamento automático da instância do BD. Você não pode definir o limite máximo de armazenamento para instâncias com dimensionamento automático habilitado para um valor maior que o armazenamento máximo alocado.

Pergunta 16

Um estúdio de Hollywood está planejando uma série de eventos promocionais que levarão ao lançamento do trailer de seu próximo thriller de ficção científica. Os executivos do estúdio querem criar um site estático com muitas animações alinhadas ao tema do filme. O estúdio contratou você como arquiteto de soluções para construir uma solução escalável sem servidor.

Qual das opções a seguir representa a solução MAIS econômica e de alto desempenho?

R: Crie o site como um site estático hospedado no Amazon S3. Crie uma distribuição do Amazon CloudFront com o Amazon S3 como origem. Use o Amazon Route 53 para criar um registro de alias que aponte para sua distribuição do Amazon CloudFront

Opção correta:

Crie o site como um site estático hospedado no Amazon S3. Crie uma distribuição do Amazon CloudFront com o Amazon S3 como origem. Use o Amazon Route 53 para criar um registro de alias que aponte para sua distribuição do Amazon CloudFront

Você pode usar o Amazon S3 para hospedar um site estático. Em um site estático, páginas da web individuais incluem conteúdo estático. Elas também podem conter scripts do lado do cliente. Para hospedar um site estático no Amazon S3, você configura um bucket do Amazon S3 para hospedagem de site e então carrega o conteúdo do seu site para o bucket.

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

Você pode usar o Amazon CloudFront para melhorar o desempenho do seu site. O CloudFront disponibiliza os arquivos do seu site (como HTML, imagens e vídeo) de data centers ao redor do mundo (chamados de edge locations). Quando um visitante solicita um arquivo do seu site, o CloudFront redireciona automaticamente a solicitação para uma cópia do arquivo no edge location mais próximo. Isso resulta em tempos de download mais rápidos do que se o visitante tivesse solicitado o conteúdo de um data center localizado mais distante. Portanto, essa opção está correta.

Pergunta 17

Você gostaria de montar um sistema de arquivos de rede em instâncias Linux, onde os arquivos serão armazenados e acessados com frequência no início, e depois com pouca frequência. Qual solução é a MAIS econômica?
R: Acesso pouco frequente do Amazon EFS

Opção correta:

Acesso pouco frequente do Amazon EFS
O Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos NFS elástico, simples, escalável e totalmente gerenciado para uso com serviços da AWS Cloud e recursos locais. O Amazon EFS é um serviço regional que armazena dados dentro e entre várias Zonas de Disponibilidade (AZs) para alta disponibilidade e durabilidade.
O Amazon EFS Infrequent Access (EFS IA) é uma classe de armazenamento que fornece preço/desempenho otimizado em termos de custo para arquivos não acessados todos os dias, com preços de armazenamento até 92% mais baixos em comparação ao Amazon EFS Standard. Portanto, esta é a opção correta.
Como funciona o Amazon EFS:

- 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. A classe de armazenamento Amazon S3 Intelligent-Tiering foi projetada para otimizar custos movendo dados automaticamente para o nível de acesso mais econômico, sem impacto no desempenho ou sobrecarga operacional. Ele funciona armazenando objetos em dois níveis de acesso: um nível otimizado para acesso frequente e outro nível de menor custo otimizado para acesso pouco frequente.
Não é possível montar um sistema de arquivos de rede no Amazon S3 Intelligent Tiering, pois ele é um serviço de armazenamento de objetos, portanto, esta opção está incorreta.

Pergunta 18

Após uma revisão de segurança da sua conta AWS, um consultor da AWS descobriu que alguns bancos de dados do Amazon RDS não estão criptografados. Como um Solutions Architect, quais etapas devem ser seguidas para criptografar os bancos de dados do Amazon RDS?
R: Tire um snapshot do banco de dados, copie-o como um snapshot criptografado e restaure um banco de dados do snapshot criptografado. Encerre o banco de dados anterior

Opção correta:

Tire um snapshot do banco de dados, copie-o como um snapshot criptografado e restaure um banco de dados do snapshot criptografado. Encerre o banco de dados anterior
O Amazon Relational Database Service (Amazon RDS) facilita a configuração, operação e dimensionamento de um banco de dados relacional na nuvem. Ele fornece capacidade redimensionável e com boa relação custo-benefício, ao mesmo tempo em que automatiza tarefas administrativas demoradas, como provisionamento de hardware, configuração de banco de dados, aplicação de patches e backups.

Você pode criptografar suas instâncias e snapshots do Amazon RDS DB em repouso habilitando a opção de criptografia para suas instâncias do Amazon RDS DB. Os dados criptografados em repouso incluem o armazenamento subjacente para instâncias do DB, seus backups automatizados, réplicas de leitura e snapshots.
Você só pode habilitar a criptografia para uma instância de banco de dados do Amazon RDS quando criá-la, não depois que a instância de banco de dados for criada. No entanto, como você pode criptografar uma cópia de um snapshot de banco de dados não criptografado, você pode efetivamente adicionar criptografia a uma instância de banco de dados não criptografada. Ou seja, você pode criar um snapshot da sua instância de banco de dados e, em seguida, criar uma cópia criptografada desse snapshot. Então, esta é a opção correta.

Pergunta 19

Um aplicativo de e-commerce usa uma implantação Amazon Aurora Multi-AZ para seu banco de dados. Ao analisar as métricas de desempenho, a equipe de engenharia descobriu que as leituras do banco de dados estão causando alta entrada/saída (E/S) e adicionando latência às solicitações de gravação no banco de dados.

Como AWS Certified Solutions Architect Associate, o que você recomendaria para separar as solicitações de leitura das solicitações de gravação?

R: Configure uma réplica de leitura e modifique o aplicativo para usar o ponto de extremidade apropriado

Opção correta:

Configure uma réplica de leitura e modifique o aplicativo para usar o ponto de extremidade apropriado
Um cluster de banco de dados do Amazon Aurora consiste em uma ou mais instâncias de banco de dados e um volume de cluster que gerencia os dados para essas instâncias de banco de dados. Um volume de cluster do Aurora é um volume de armazenamento de banco de dados virtual que abrange várias Zonas de Disponibilidade (AZs), com cada Zona de Disponibilidade (AZ) tendo uma cópia dos dados do cluster de banco de dados. Dois tipos de instâncias de banco de dados compõem um cluster de banco de dados do Aurora:
Instância de BD primária – Suporta operações de leitura e gravação, e realiza todas as modificações de dados no volume do cluster. Cada cluster de BD Aurora tem uma instância de BD primária.
Aurora Replica – Conecta-se ao mesmo volume de armazenamento que a instância primária do BD e suporta apenas operações de leitura. Cada cluster Aurora DB pode ter até 15 Aurora Replicas além da instância primária do BD. O Aurora faz failover automaticamente para uma Aurora Replica caso a instância primária do BD fique indisponível. Você pode especificar a prioridade de failover para Aurora Replicas. Aurora Replicas também pode descarregar cargas de trabalho de leitura da instância primária do BD.

As réplicas do Aurora têm dois propósitos principais. Você pode emitir consultas a elas para dimensionar as operações de leitura para seu aplicativo. Normalmente, você faz isso conectando-se ao ponto de extremidade do leitor do cluster. Dessa forma, o Aurora pode distribuir a carga para conexões somente leitura em quantas réplicas do Aurora você tiver no cluster. As réplicas do Aurora também ajudam a aumentar a disponibilidade. Se a instância do gravador em um cluster ficar indisponível, o Aurora promove automaticamente uma das instâncias do leitor para tomar seu lugar como o novo gravador. Ao configurar uma implantação Multi-AZ para o Aurora, você cria uma réplica do Aurora ou um nó de leitor em uma Zona de Disponibilidade (AZ) diferente.

Você usa o endpoint do leitor para conexões somente leitura para seu cluster Aurora. Esse endpoint usa um mecanismo de balanceamento de carga para ajudar seu cluster a lidar com uma carga de trabalho intensiva em consultas. O endpoint do leitor é o endpoint que você fornece para aplicativos que fazem relatórios ou outras operações somente leitura no cluster. O endpoint do leitor balanceia a carga de conexões para réplicas do Aurora disponíveis em um cluster de banco de dados do Aurora.

Pergunta 20

Uma empresa de manufatura recebe um serviço não confiável de seu provedor de data center porque a empresa está localizada em uma área propensa a desastres naturais. A empresa não está pronta para migrar totalmente para a Nuvem AWS, mas quer um ambiente de failover na AWS caso o data center local falhe. A empresa executa servidores web que se conectam a fornecedores externos. Os dados disponíveis na AWS e no local devem ser uniformes.

Qual das seguintes soluções teria a MENOR quantidade de tempo de inatividade?

R: Configurar um registro de failover do Amazon Route 53. Executar servidores de aplicativos em instâncias do Amazon EC2 por trás de um Application Load Balancer em um grupo de Auto Scaling. Configurar o AWS Storage Gateway com volumes armazenados para fazer backup de dados no Amazon S3

Opção correta:

Configurar um registro de failover do Amazon Route 53. Executar servidores de aplicativos em instâncias do Amazon EC2 por trás de um Application Load Balancer em um grupo de Auto Scaling. Configurar o AWS Storage Gateway com volumes armazenados para fazer backup de dados no Amazon S3

Se você tiver vários recursos que executam a mesma função, poderá configurar o failover de DNS para que o Route 53 roteie seu tráfego de um recurso não íntegro para um recurso íntegro.

O Elastic Load Balancing é usado para distribuir automaticamente o tráfego de entrada do seu aplicativo em todas as instâncias do Amazon EC2 que você está executando. Você pode usar o Elastic Load Balancing para gerenciar solicitações de entrada roteando o tráfego de forma otimizada para que nenhuma instância fique sobrecarregada. Seu balanceador de carga atua como um único ponto de contato para todo o tráfego da web de entrada para seu grupo de Auto Scaling.

O AWS Storage Gateway é um serviço de armazenamento em nuvem híbrido que fornece acesso local a armazenamento em nuvem praticamente ilimitado. Ele fornece desempenho de baixa latência ao armazenar em cache dados acessados com frequência no local, enquanto armazena dados de forma segura e durável nos serviços de armazenamento em nuvem da Amazon. O Storage Gateway otimiza a transferência de dados para a AWS enviando apenas dados alterados e compactando dados. O Storage Gateway também se integra nativamente ao armazenamento em nuvem Amazon S3, o que torna seus dados disponíveis para processamento na nuvem.

Pergunta 21

Uma empresa de TI tem um aplicativo Access Control Management (ACM) que usa o Amazon RDS para MySQL, mas está enfrentando problemas de desempenho, apesar de usar Read Replicas. A empresa contratou você como arquiteto de soluções para lidar com esses desafios relacionados ao desempenho sem se afastar do esquema de banco de dados relacional subjacente. A empresa tem filiais em todo o mundo e precisa que a solução funcione em escala global.

Qual das seguintes opções você recomendaria como a solução MAIS econômica e de alto desempenho?

R: Use o Amazon Aurora Global Database para habilitar leituras locais rápidas com baixa latência em cada região

Opção correta:

Use o Amazon Aurora Global Database para habilitar leituras locais rápidas com baixa latência em cada região

O Amazon Aurora é um banco de dados relacional compatível com MySQL e PostgreSQL criado para a nuvem, que combina o desempenho e a disponibilidade de bancos de dados empresariais tradicionais com a simplicidade e a relação custo-benefício de bancos de dados de código aberto. O Amazon Aurora apresenta um sistema de armazenamento distribuído, tolerante a falhas e auto-reparável que dimensiona automaticamente até 64 TB por instância de banco de dados. O

Aurora não é um banco de dados na memória.
O Amazon Aurora Global Database foi projetado para aplicativos distribuídos globalmente, permitindo que um único banco de dados Amazon Aurora abranja várias regiões da AWS. Ele replica seus dados sem impacto no desempenho do banco de dados, permite leituras locais rápidas com baixa latência em cada região e fornece recuperação de desastres de interrupções em toda a região. O Amazon Aurora Global Database é a escolha correta para o caso de uso fornecido.

Pergunta 22

Qual das seguintes políticas do IAM fornece acesso somente leitura ao bucket do Amazon S3 `mybucket`e seu conteúdo?

Opção correta:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":"arn:aws:s3:::mybucket"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"arn:aws:s3:::mybucket/*"
      }
   ]
}
```

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

`s3:ListBucket`é aplicado aos buckets, então o ARN está no formato `"Resource":"arn:aws:s3:::mybucket"`, sem um final para indicar todos os objetos dentro do `/` `s3:GetObject`bucket`"Resource":"arn:aws:s3:::mybucket/*"/*mybucket`

Pergunta 23

Uma empresa de serviços financeiros desenvolveu seu aplicativo principal na AWS Cloud com requisitos de segurança de dados, de modo que a chave de criptografia deve ser armazenada em um aplicativo personalizado em execução no local. A empresa quer descarregar o armazenamento de dados, bem como o processo de criptografia para o Amazon S3, mas continuar a usar a chave de criptografia existente.

Qual das seguintes opções de criptografia do Amazon S3 permite que a empresa utilize o Amazon S3 para armazenar dados com determinadas restrições?

R: Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Opção correta:

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Você tem as seguintes opções para proteger dados em repouso no Amazon S3:

Criptografia do lado do servidor – solicite ao Amazon S3 para criptografar seu objeto antes de salvá-lo em discos em seus data centers e, em seguida, descriptografá-lo quando você baixar os objetos.

Criptografia do lado do cliente – Criptografe dados do lado do cliente e carregue os dados criptografados para o Amazon S3. Neste caso, você gerencia o processo de criptografia, as chaves de criptografia e as ferramentas relacionadas.

Para o caso de uso fornecido, a empresa deseja gerenciar as chaves de criptografia por meio de seu aplicativo personalizado e deixar que o Amazon S3 gerencie a criptografia; portanto, você deve usar a Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).

Pergunta 24

Você está estabelecendo uma solução de monitoramento para sistemas de desktop, que enviará dados de telemetria para a AWS a cada 1 minuto. Os dados de cada sistema devem ser processados em ordem, independentemente, e você gostaria de dimensionar o número de consumidores para ser possivelmente igual ao número de sistemas de desktop que estão sendo monitorados.

O que você recomenda?

R: Use uma fila FIFO (First-In-First-Out) do Amazon Simple Queue Service (Amazon SQS) e certifique-se de que os dados de telemetria sejam enviados com um atributo de ID de grupo que representa o valor do ID da área de trabalho

Opção correta:

Use uma fila FIFO (First-In-First-Out) do Amazon Simple Queue Service (Amazon SQS) e certifique-se de que os dados de telemetria sejam enviados com um atributo de ID de grupo que representa o valor do ID da área de trabalho

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

Portanto, precisamos usar uma fila FIFO SQS. Se não especificarmos um GroupID, todas as mensagens estarão em ordem absoluta, mas podemos ter apenas 1 consumidor no máximo. Para permitir que vários consumidores leiam dados para cada aplicativo Desktop e para dimensionar o número de consumidores, devemos usar o atributo "Group ID". Portanto, esta é a opção correta.

Pergunta 25

Você gostaria de armazenar uma senha de banco de dados em um local seguro e habilitar a rotação automática dessa senha a cada 90 dias. O que você recomenda?

R: Gerenciador de segredos da AWS

Opção correta:

Gerenciador de segredos da AWS

O AWS Secrets Manager ajuda você a proteger os segredos necessários para acessar seus aplicativos, serviços e recursos de TI. O serviço permite que você gire, gerencie e recupere facilmente credenciais de banco de dados, chaves de API e outros segredos ao longo de seu ciclo de vida. Usuários e aplicativos recuperam segredos com uma chamada para APIs do Secrets Manager, eliminando a necessidade de codificar informações confidenciais em texto simples. O Secrets Manager oferece rotação de segredos com integração interna para Amazon RDS, Amazon Redshift e Amazon DocumentDB. A resposta correta aqui é Secrets Manager

Pergunta 26

Uma empresa de consultoria de big data precisa configurar um data lake no Amazon S3 para um cliente de assistência médica. O data lake é dividido em zonas brutas e refinadas. Por motivos de conformidade, os dados de origem precisam ser mantidos por no mínimo 5 anos. Os dados de origem chegam na zona bruta e são processados por meio de um trabalho de extração, transformação e carregamento (ETL) baseado no AWS Glue na zona refinada. Os analistas de negócios executam consultas ad-hoc apenas nos dados na zona refinada usando o Amazon Athena. A equipe está preocupada com o custo do armazenamento de dados nas zonas brutas e refinadas, pois os dados estão aumentando a uma taxa de 1 terabyte por dia em cada zona.

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

(Selecione duas)

R: Use o trabalho ETL do AWS Glue para gravar os dados transformados na zona refinada usando um formato de arquivo compactado

R: Configurar uma política de ciclo de vida para fazer a transição dos dados da zona bruta para o Amazon S3 Glacier Deep Archive após 1 dia da criação do objeto

Opções corretas:

Configurar uma política de ciclo de vida para fazer a transição dos dados da zona bruta para o Amazon S3 Glacier Deep Archive após 1 dia da criação do objeto

Você pode gerenciar seus objetos para que eles sejam armazenados de forma econômica durante todo o ciclo de vida configurando o Amazon S3 Lifecycle. Uma configuração do S3 Lifecycle é um conjunto de regras que definem ações que o Amazon S3 aplica a um grupo de objetos. Por exemplo, você pode escolher fazer a transição de objetos para a classe de armazenamento Amazon S3 Standard-IA 30 dias após criá- los ou arquivá-los na classe de armazenamento Amazon S3 Glacier um ano após criá-los. Para o caso de uso fornecido, a zona bruta consiste nos dados de origem, portanto, não pode ser excluída devido a motivos de conformidade. Portanto, você deve usar uma política de ciclo de vida para fazer a transição dos dados da zona bruta para o Amazon S3 Glacier Deep Archive após 1 dia da criação do objeto.

Use o trabalho ETL do AWS Glue para gravar os dados transformados na zona refinada usando um formato de arquivo compactado

O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado que facilita para os clientes preparar e carregar seus dados para análise. Você não pode fazer a transição dos dados de zona refinados para o Amazon S3 Glacier Deep Archive porque eles são usados pelos analistas de negócios para consultas ad-hoc. Portanto, a melhor otimização é ter os dados de zona refinados armazenados em um formato compactado por meio do trabalho do Glue. Os dados compactados reduziriam o custo de armazenamento incorrido nos dados na zona refinada.

Veja este exemplo de um pipeline ETL do AWS Glue:

Pergunta 27

Um administrador de sistemas criou uma zona hospedada privada e a associou a uma Virtual Private Cloud (VPC). No entanto, as consultas do Domain Name System (DNS) para a zona hospedada privada permanecem

sem solução.

Como arquiteto de soluções, você pode identificar as opções da Amazon Virtual Private Cloud (Amazon VPC) a serem configuradas para que a zona hospedada privada funcione?

R: Habilitar nomes de host DNS e resolução DNS para zonas hospedadas privadas

Opção correta:

Habilitar nomes de host DNS e resolução DNS para zonas hospedadas privadas

Nomes de host DNS e resolução DNS são configurações necessárias para zonas hospedadas privadas. Consultas DNS para zonas hospedadas privadas podem ser resolvidas somente pelo servidor DNS VPC fornecido pela Amazon. Como resultado, essas opções devem ser habilitadas para que sua zona hospedada privada funcione.

Nomes de host DNS: para nuvens privadas virtuais não padrão que não são criadas usando o assistente do Amazon VPC, esta opção é desabilitada por padrão. Se você criar uma zona hospedada privada para um domínio e criar registros na zona sem habilitar nomes de host DNS, as zonas hospedadas privadas não serão habilitadas. Para usar uma zona hospedada privada, esta opção deve ser habilitada.

Resolução de DNS: Zonas hospedadas privadas aceitam consultas DNS somente de um servidor DNS VPC. O endereço IP do servidor DNS VPC é o endereço IP reservado na base do intervalo de rede IPv4 VPC mais dois. Habilitar a resolução de DNS permite que você use o servidor DNS VPC como um Resolver para executar a resolução de DNS. Mantenha esta opção desabilitada se estiver usando um servidor DNS personalizado no conjunto de Opções de DHCP e não estiver usando uma zona hospedada privada.

Pergunta 28

Uma empresa está procurando armazenar seus arquivos acessados com menos frequência na AWS que podem ser acessados simultaneamente por centenas de instâncias do Amazon EC2. A empresa precisa do serviço de armazenamento de arquivos mais econômico que forneça acesso imediato aos dados sempre que necessário.

Qual das seguintes opções representa a melhor solução para os requisitos fornecidos?

R: Amazon Elastic File System (EFS) Standard–classe de armazenamento IA

Opção correta:

Amazon Elastic File System (EFS) Standard–IA storage class

- Amazon EFS é um serviço de armazenamento de arquivos para uso com Amazon Compute (EC2, contêineres, serverless) e servidores locais. O Amazon EFS fornece uma interface de sistema de arquivos, semântica de acesso ao sistema de arquivos (como consistência forte e bloqueio de arquivos) e armazenamento acessível simultaneamente para até milhares de instâncias do Amazon EC2.

A classe de armazenamento Amazon S3 Standard–IA reduz os custos de armazenamento para arquivos que não são acessados todos os dias. Ela faz isso sem sacrificar a alta disponibilidade, alta durabilidade, elasticidade e acesso ao sistema de arquivos POSIX que o Amazon EFS fornece. A AWS recomenda o armazenamento Standard-IA se você precisa que seu conjunto de dados completo seja facilmente acessível e deseja economizar automaticamente em custos de armazenamento para arquivos que são acessados com menos frequência.

Pergunta 29

Um grupo de pesquisa de Machine Learning usa um aplicativo de visão computacional proprietário hospedado em uma instância do Amazon EC2. Toda vez que a instância precisa ser parada e iniciada novamente, o aplicativo leva cerca de 3 minutos para iniciar, pois alguns programas de software auxiliares precisam ser executados para que o aplicativo possa funcionar. O grupo de pesquisa gostaria de minimizar o tempo de boostrap do aplicativo sempre que o sistema precisar ser parado e iniciado posteriormente.

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

R: Usar a hibernação da instância do Amazon EC2

Opção correta:

Usar a hibernação da instância do Amazon EC2
Quando você hiberna uma instância, a AWS sinaliza ao sistema operacional para executar a hibernação (suspensão para disco). A hibernação salva o conteúdo da memória da instância (RAM) no seu volume raiz do Amazon EBS. A AWS então persiste o volume raiz do Amazon EBS da instância e quaisquer volumes de dados do Amazon EBS anexados.
Ao iniciar sua instância:
O volume raiz do Amazon EBS é restaurado ao seu estado anterior
O conteúdo da RAM é recarregado
Os processos que estavam em execução anteriormente na instância são retomados
Os volumes de dados anexados anteriormente são anexados novamente e a instância mantém seu ID de instância

Ao usar a hibernação do Amazon EC2, temos a capacidade de retomá-la a qualquer momento, com o aplicativo já iniciado, o que nos ajuda a reduzir o tempo de inicialização de 3 minutos.

Pergunta 30

Uma equipe de engenharia quer examinar a viabilidade do user datarecurso do Amazon EC2 para um projeto futuro.
Quais das seguintes opções são verdadeiras sobre a configuração de dados do usuário do Amazon EC2?

(Selecione duas)
R: Por padrão, os scripts inseridos como dados do usuário são executados com privilégios de usuário root
R: Por padrão, os dados do usuário são executados apenas durante o ciclo de inicialização quando você inicia uma instância pela primeira vez

Opções corretas:

Os Dados do Usuário geralmente são usados para executar tarefas comuns de configuração automatizada e até mesmo executar scripts após a instância iniciar. Ao iniciar uma instância no Amazon EC2, você pode passar dois tipos de dados do usuário - scripts de shell e diretivas cloud-init. Você também pode passar esses dados para o assistente de inicialização como texto simples ou como um arquivo.

Por padrão, os scripts inseridos como dados do usuário são executados com privilégios de usuário root
Scripts inseridos como dados do usuário são executados como o usuário root, portanto não precisam do comando sudo no script. Quaisquer arquivos que você criar serão de propriedade do root; se você precisar que usuários não root tenham acesso ao arquivo, você deve modificar as permissões de acordo no script.

Por padrão, os dados do usuário são executados apenas durante o ciclo de inicialização quando você inicia uma instância pela primeira vez
Por padrão, os scripts de dados do usuário e as diretivas cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. Você pode atualizar sua configuração para garantir que seus scripts de dados do usuário e as diretivas cloud-init sejam executados sempre que você reiniciar sua instância.

Pergunta 31

O Amazon EC2 Auto Scaling precisa encerrar uma instância da Zona de Disponibilidade (AZ), us-east-1apois ela tem o maior número de instâncias entre as Zonas de Disponibilidade (AZs) sendo usadas

atualmente. Há 4 instâncias na Zona de Disponibilidade (AZ) us-east-1a, assim: a Instância A tem o modelo de inicialização mais antigo, a Instância B tem a configuração de inicialização mais antiga, a Instância C tem a configuração de inicialização mais recente e a Instância D está mais próxima da próxima hora de cobrança.

Qual das seguintes instâncias seria encerrada de acordo com a política de encerramento padrão?

R: Instância B

Opção correta:

Instância B

De acordo com a política de término padrão, a primeira prioridade é dada a qualquer estratégia de alocação para instâncias On-Demand vs Spot. Como nenhuma informação desse tipo foi fornecida para o caso de uso fornecido, esse critério pode ser ignorado. A próxima prioridade é considerar qualquer instância com o modelo de inicialização mais antigo, a menos que haja uma instância que use uma configuração de inicialização. Portanto, isso descarta a Instância A. Em seguida, você precisa considerar qualquer instância que tenha a configuração de inicialização mais antiga. Isso implica que a Instância B será selecionada para término e a Instância C também será descartada, pois tem a configuração de inicialização mais recente. A Instância D, que está mais próxima da próxima hora de cobrança, não é selecionada, pois esse critério é o último na ordem de prioridade.

Pergunta 32

A equipe de engenharia de uma empresa de comércio eletrônico está trabalhando em otimizações de custo para instâncias do Amazon Elastic Compute Cloud (Amazon EC2). A equipe quer gerenciar a carga de trabalho usando uma mistura de instâncias on-demand e spot em vários tipos de instância. Eles gostariam de criar um grupo de Auto Scaling com uma mistura dessas instâncias.

Qual das seguintes opções permitiria à equipe de engenharia provisionar as instâncias para este caso de uso?

R: Você só pode usar um modelo de inicialização para provisionar capacidade em vários tipos de instância usando instâncias sob demanda e instâncias spot para atingir a escala, o desempenho e o custo desejados.

Opção correta:

Você só pode usar um modelo de inicialização para provisionar capacidade em vários tipos de instância usando instâncias sob demanda e instâncias spot para atingir a escala, o desempenho e o custo desejados.

Um modelo de inicialização é semelhante a uma configuração de inicialização, pois especifica informações de configuração de instância, como o ID da Amazon Machine Image (AMI), o tipo de instância, um par de chaves, grupos de segurança e outros parâmetros que você usa para iniciar instâncias do EC2. Além disso, definir um modelo de inicialização em vez de uma configuração de inicialização permite que você tenha várias versões de um modelo.

Com modelos de lançamento, você pode provisionar capacidade em vários tipos de instância usando Instâncias On-Demand e Instâncias Spot para atingir a escala, o desempenho e o custo desejados. Portanto, esta é a opção correta.

Pergunta 33

Uma empresa de consultoria de big data está trabalhando em um contrato com um cliente em que as cargas de trabalho de extração, transformação e carregamento (ETL) são atualmente manipuladas por meio de um cluster Hadoop implantado no data center local. O cliente deseja migrar suas cargas de trabalho de ETL para a AWS Cloud. A solução AWS Cloud precisa estar altamente disponível com cerca de 50 instâncias do Amazon Elastic Compute Cloud (Amazon EC2) por Availability Zone (AZ).

Como arquiteto de soluções, qual dos seguintes grupos de posicionamento do Amazon EC2 você recomendaria para lidar com a carga de trabalho de ETL distribuída?

R: Grupo de posicionamento de partição

Opção correta:

Grupo de posicionamento de partição

Você pode usar grupos de posicionamento para influenciar o posicionamento de um grupo de instâncias interdependentes para atender às necessidades da sua carga de trabalho. Dependendo do tipo de carga de trabalho, você pode criar um grupo de posicionamento usando uma das seguintes estratégias de posicionamento:

Grupo de posicionamento de partição – espalha suas instâncias em partições lógicas de modo que grupos de instâncias em uma partição não compartilhem o hardware subjacente com grupos de instâncias em partições diferentes. Essa estratégia é normalmente usada por grandes cargas de trabalho distribuídas e replicadas, como Hadoop, Cassandra e Kafka. Portanto, essa é a opção correta para o caso de uso fornecido.

Pergunta 34

Um desenvolvedor configurou o tráfego de entrada para as portas relevantes tanto no Security Group da instância do Amazon EC2 quanto na lista de controle de acesso à rede (network ACL) da sub-rede para a instância do Amazon EC2. O desenvolvedor, no entanto, não consegue se conectar ao serviço em execução na instância do Amazon EC2.

Como arquiteto de soluções, como você resolverá esse problema?

R: Os grupos de segurança são stateful, então permitir tráfego de entrada para as portas necessárias habilita a conexão. A lista de controle de acesso à rede (ACL de rede) é stateless, então você deve permitir tráfego de entrada e saída

Opção correta:

Os grupos de segurança são stateful, então permitir tráfego de entrada para as portas necessárias habilita a conexão. A lista de controle de acesso à rede (ACL de rede) é stateless, então você deve permitir tráfego de entrada e saída

Os grupos de segurança são stateful, então permitir tráfego de entrada para as portas necessárias habilita a conexão. As ACLs de rede são stateless, então você deve permitir tráfego de entrada e saída.

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

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

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

Se você aceitar tráfego da internet, então você também deve estabelecer uma rota através de um gateway de internet. Se você aceitar tráfego por VPN ou AWS Direct Connect, então você deve estabelecer uma rota através de um gateway privado virtual.

Pergunta 35

Para melhorar o desempenho e a segurança do aplicativo, a equipe de engenharia de uma empresa criou uma distribuição do Amazon CloudFront com um Application Load Balancer como origem personalizada. A equipe também configurou um AWS Web Application Firewall (AWS WAF) com distribuição do Amazon CloudFront. A equipe de segurança da empresa notou um aumento nos ataques maliciosos de um endereço IP

específico para roubar dados confidenciais armazenados nas instâncias do Amazon EC2.

Como arquiteto de soluções, qual das seguintes ações você recomendaria para interromper os ataques?

R: Crie uma condição de correspondência de IP no AWS WAF para bloquear o endereço IP malicioso

Opção correta:

Crie uma condição de correspondência de IP no AWS WAF para bloquear o endereço IP malicioso

O AWS WAF é um firewall de aplicativo da Web que ajuda a proteger seus aplicativos da Web ou APIs contra explorações comuns da Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. O AWS WAF oferece controle sobre como o tráfego chega aos seus aplicativos, 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 define.

Se você quiser permitir ou bloquear solicitações da web com base nos endereços IP dos quais as solicitações se originam, crie uma ou mais condições de correspondência de IP. Uma condição de correspondência de IP lista até 10.000 endereços IP ou intervalos de endereços IP dos quais suas solicitações se originam. Então, essa opção está correta.

Pergunta 36

Um aplicativo da web de compartilhamento de fotos sociais é hospedado em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) por trás de um Elastic Load Balancer. O aplicativo dá aos usuários a capacidade de carregar suas fotos e também mostra um placar na página inicial do aplicativo. As fotos carregadas são armazenadas no Amazon Simple Storage Service (Amazon S3) e os dados do placar são mantidos no Amazon DynamoDB. As instâncias do Amazon EC2 precisam acessar o Amazon S3 e o Amazon DynamoDB para esses recursos.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria como a opção MAIS segura?

R: Anexe a função IAM apropriada ao perfil da instância do Amazon EC2 para que a instância possa acessar o Amazon S3 e o Amazon DynamoDB

Opção correta:

Anexe a função IAM apropriada ao perfil da instância do Amazon EC2 para que a instância possa acessar o Amazon S3 e o Amazon DynamoDB

Os aplicativos que são executados em uma instância do Amazon EC2 devem incluir credenciais da AWS em suas solicitações de API da AWS. Você pode fazer com que seus desenvolvedores armazenem credenciais da AWS diretamente na instância do Amazon EC2 e permitam que os aplicativos nessa instância usem essas credenciais. Mas os desenvolvedores teriam que gerenciar as credenciais e garantir que eles as transmitissem com segurança para cada instância e atualizassem cada instância do Amazon EC2 quando fosse o momento de rotacionar as credenciais.

Em vez disso, você deve usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que são executados em uma instância do Amazon EC2. Ao usar uma função, você não precisa distribuir credenciais de longo prazo (como um nome de usuário e senha ou chaves de acesso) para uma instância do Amazon EC2. A função fornece permissões temporárias que os aplicativos podem usar quando fazem chamadas para outros recursos da AWS. Ao iniciar uma instância do Amazon EC2, você especifica uma função do IAM para associar à instância. Os aplicativos que são executados na instância podem usar as credenciais temporárias fornecidas pela função para assinar solicitações de API. Portanto, esta opção está correta.

Pergunta 37

Uma startup baseada no Vale do Silício tem um aplicativo de gerenciamento de conteúdo com a camada da web em execução em instâncias do Amazon EC2 e a camada do banco de dados em execução no Amazon Aurora. Atualmente, toda a infraestrutura está localizada na us-east-1região. A startup tem 90% de seus clientes nos EUA e na Europa. A equipe de engenharia está recebendo relatórios de desempenho de aplicativo deteriorado de clientes na Europa com alto tempo de carregamento de aplicativo.

Como arquiteto de soluções, qual das seguintes opções você recomendaria para resolver esses problemas de desempenho? (Selecione duas)

R: Crie réplicas de leitura do Amazon Aurora na `eu-west-1` região

R: Configure outra frota de instâncias do Amazon EC2 para a camada da web na `eu-west-1` região. Habilite a política de roteamento de latência no Amazon Route 53

Opções corretas:

Configure outra frota de instâncias do Amazon EC2 para a camada da web na `eu-west-1` região. Habilite a política de roteamento de latência no Amazon Route 53

O Amazon Route 53 é um serviço web Domain Name System (DNS) em nuvem altamente disponível e escalável. Use o roteamento baseado em latência quando tiver recursos em várias regiões da AWS e quiser rotear o tráfego para a região que fornece a menor latência. Para usar o roteamento baseado em latência, crie registros de latência para seus recursos em várias regiões da AWS. Quando o Amazon Route 53 recebe uma consulta DNS para seu domínio ou subdomínio (example.com ou acme.example.com), ele determina para quais regiões da AWS você criou registros de latência, determina qual região fornece ao usuário a menor latência e, em seguida, seleciona um registro de latência para essa região. O Route 53 responde com o valor do registro selecionado, como o endereço IP de um servidor web.

Como os clientes na Europa estão enfrentando problemas de desempenho com alto tempo de carregamento de aplicativos, você pode usar roteamento baseado em latência para reduzir a latência.

Crie réplicas de leitura do Amazon Aurora na `eu-west-1` região

O Amazon Aurora é um banco de dados relacional compatível com MySQL e PostgreSQL criado para a nuvem, que combina o desempenho e a disponibilidade de bancos de dados empresariais tradicionais com a simplicidade e a relação custo-benefício de bancos de dados de código aberto. O Amazon Aurora apresenta um sistema de armazenamento distribuído, tolerante a falhas e auto-reparável que dimensiona automaticamente até 64 TB por instância de banco de dados.

Réplicas de leitura do Amazon Aurora podem ser usadas para escalar leituras entre regiões. Isso melhorará o desempenho do aplicativo para usuários na Europa. Portanto, essa também é uma opção correta para o caso de uso fornecido.

Pergunta 38

Uma empresa de TI quer otimizar os custos incorridos em sua frota de 100 instâncias do Amazon EC2 para o próximo ano. Com base em análises históricas, a equipe de engenharia observou que 70 dessas instâncias lidam com os serviços de computação de seu aplicativo principal e precisam estar sempre disponíveis. As outras 30 instâncias são usadas para lidar com trabalhos em lote que podem gerar um atraso no processamento.

Como arquiteto de soluções, qual das seguintes opções você recomendaria como a solução com melhor custo-benefício?

R: Compre 70 instâncias reservadas (RIs) e 30 instâncias spot

Opção correta:

Compre 70 instâncias reservadas (RIs) e 30 instâncias spot

Como 70 instâncias precisam estar sempre disponíveis, elas podem ser compradas como instâncias reservadas por um período de um ano. As outras 30 instâncias responsáveis pelo trabalho em lote podem ser compradas como instâncias spot. Mesmo que algumas das instâncias spot sejam interrompidas, outras instâncias spot podem continuar com o trabalho.
Veja esta visão geral detalhada de vários tipos de instâncias do Amazon EC2 de uma perspectiva de preço.

Pergunta 39

O que é verdade sobre a criptografia de réplicas de leitura do Amazon RDS?
R: Se o banco de dados mestre estiver criptografado, as réplicas de leitura serão criptografadas

Opção correta:

Se o banco de dados mestre estiver criptografado, as réplicas de leitura serão criptografadas
As réplicas de leitura do Amazon RDS fornecem desempenho e durabilidade aprimorados para instâncias de banco de dados (DB) RDS. Elas facilitam o dimensionamento elástico além das restrições de capacidade de uma única instância de banco de dados para cargas de trabalho de banco de dados com leitura pesada. 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 instantâneo 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 de banco de dados de origem. As réplicas de leitura podem estar dentro de uma zona de disponibilidade, entre AZs ou entre regiões.
Em uma instância de banco de dados em execução com criptografia Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados, assim como seus backups automatizados, réplicas de leitura e snapshots. Portanto, esta opção está correta.

Pergunta 40

Uma empresa historicamente operou apenas na us-east-1região e armazena dados criptografados no Amazon S3 usando SSE-KMS. Como parte do aprimoramento de sua postura de segurança, bem como da melhoria da arquitetura de backup e recuperação, a empresa deseja armazenar os dados criptografados no Amazon S3 que são replicados na us-west-1região da AWS. As políticas de segurança determinam que os dados devem ser criptografados e descriptografados usando a mesma chave em ambas as regiões da AWS.
Qual das seguintes opções representa a melhor solução para atender a esses requisitos?
R: Crie um novo bucket do Amazon S3 na `us-east-1` região com replicação habilitada deste novo bucket para outro bucket na `us-west-1` região. Habilite a criptografia SSE-KMS no novo bucket na `us-east-1` região usando uma chave multirregional do AWS KMS. Copie os dados existentes do bucket atual do Amazon S3 na `us-east-1` região para este novo bucket do Amazon S3 na `us-east-1` região

Opção correta:

Crie um novo bucket do Amazon S3 na `us-east-1` região com replicação habilitada deste novo bucket para outro bucket na `us-west-1` região. Habilite a criptografia SSE-KMS no novo bucket na `us-east-1` região usando uma chave multirregional do AWS KMS. Copie os dados existentes do bucket atual do Amazon S3 na `us-east-1` região para este novo bucket do Amazon S3 na `us-east-1` região
O AWS KMS oferece suporte a chaves multirregionais, que são chaves do AWS KMS em diferentes regiões da AWS que podem ser usadas de forma intercambiável, como se você tivesse a mesma chave em várias regiões. Cada conjunto de chaves multirregionais relacionadas tem o mesmo material de chave e ID de chave, então você pode criptografar dados em uma região da AWS e descriptografá-los em uma região diferente da AWS sem criptografar novamente ou fazer uma chamada entre regiões para o AWS KMS.
Você pode usar chaves AWS KMS multirregionais no Amazon S3. No entanto, o Amazon S3 atualmente trata chaves multirregionais como se fossem chaves de região única e não usa os recursos multirregionais da

chave.

Para o caso de uso fornecido, você deve criar um novo bucket na `us-east-1` região com replicação habilitada deste novo bucket para outro bucket na `us-west-1` região. Isso garantiria que os dados estivessem disponíveis em outra região para fins de backup e recuperação. Você também deve habilitar a criptografia SSE-KMS no novo bucket na `us-east-1` região usando uma chave multirregional do AWS KMS para que os dados possam ser criptografados e descriptografados usando a mesma chave em ambas as regiões da AWS. Como os dados existentes no bucket atual foram criptografados usando a chave AWS KMS restrita à `us-east-1` região, os dados devem ser copiados para o novo `bucket na` `us-east-1` região para replicação, bem como a criptografia baseada na chave KMS multirregional para entrar em ação.
Para exigir criptografia do lado do servidor de todos os objetos em um bucket específico do Amazon S3, você pode usar uma política. Por exemplo, a seguinte política de bucket nega a permissão de upload de objeto (s3:PutObject) para todos se a solicitação não incluir o cabeçalho x-amz-server-side-encryption solicitando criptografia do lado do servidor com SSE-KMS.

```
{
   "Version":"2012-10-17",
   "Id":"PutObjectPolicy",
   "Statement":[{
         "Sid":"DenyUnEncryptedObjectUploads",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::DOC-EXAMPLE-BUCKET1/*",
         "Condition":{
            "StringNotEquals":{
               "s3:x-amz-server-side-encryption":"aws:kms"
            }
         }
      }
   ]
}
```

Os exemplos de políticas do IAM a seguir mostram instruções para usar a criptografia do lado do servidor do AWS KMS com replicação.
Neste exemplo, o contexto de criptografia é o ARN do objeto. Se você usar o SSE-KMS com uma Amazon S3 Bucket Key habilitada, deverá usar o ARN do bucket como o contexto de criptografia.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": ["kms:Decrypt"],
            "Effect": "Allow",
            "Resource": "List of AWS KMS key ARNs used to encrypt source objects.",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.source-bucket-region.amazonaws.com",
                                                                "kms:EncryptionContext:aws:s3:arn":
"arn:aws:s3:::source-bucket-name/key-prefix1/*"
                }
            }
        },
```

```
        {
            "Action": ["kms:Encrypt"],
            "Effect": "Allow",
              "Resource": "AWS KMS key ARNs (for the AWS Region of the destination bucket 1). Used to
encrypt object replicas created in destination bucket 1.",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.destination-bucket-1-region.amazonaws.com",
                      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::destination-bucket-name-1/key-
prefix1/*"
                }
            }
        },
        {
            "Action": ["kms:Encrypt"],
            "Effect": "Allow",
               "Resource": "AWS KMS key ARNs (for the AWS Region of destination bucket 2). Used to
encrypt object replicas created in destination bucket 2.",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.destination-bucket-2-region.amazonaws.com",
                      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::destination-bucket-2-name/key-
prefix1*"
                }
            }
        }
    ]
}
```

Pergunta 41

Sua empresa implantou um aplicativo que executará muitas sobrescrições e exclusões de dados e exigirá que as informações mais recentes estejam disponíveis sempre que os dados forem lidos por meio de consultas em tabelas de banco de dados.

Como arquiteto de soluções, qual tecnologia de banco de dados você recomendaria?

R: Serviço de banco de dados relacional da Amazon (Amazon RDS)

Opção correta:

Serviço de banco de dados relacional da Amazon (Amazon RDS)

O Amazon Relational Database Service (Amazon RDS) facilita a configuração, operação e dimensionamento de um banco de dados relacional na nuvem. Ele fornece 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. O RDS permite que você crie, leia, atualize e exclua registros sem nenhum bloqueio de item ou ambiguidade. Todas as transações do RDS devem ser compatíveis com ACID ou ser Atômicas, Consistentes, Isoladas e Duráveis para garantir a integridade dos dados.

A atomicidade exige que a transação como um todo seja executada com sucesso ou, se uma parte da transação falhar, a transação inteira seja invalidada. A consistência exige que os dados gravados no banco de dados como parte da transação devem aderir a todas as regras definidas e restrições,

incluindo restrições, cascatas e gatilhos. O isolamento é crítico para atingir o controle de simultaneidade e garante que cada transação seja independente de si mesma. A durabilidade exige que todas as alterações feitas no banco de dados sejam permanentes assim que uma transação for concluída. Portanto, o melhor ajuste é o Amazon RDS.

Pergunta 42

Uma empresa de serviços financeiros deseja armazenar dados confidenciais no Amazon S3 e precisa atender às seguintes normas de segurança e conformidade de dados:

- O uso da chave de criptografia deve ser registrado para fins de auditoria
- As chaves de criptografia devem ser rotacionadas a cada ano

Os dados devem ser criptografados em repouso

Qual é a solução operacional MAIS eficiente?

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) com rotação automática de chaves

R: Criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) com rotação automática de chaves

Opção correta:

Criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) com rotação automática de chaves

Criptografia do lado do servidor é a criptografia de dados em seu destino pelo aplicativo ou serviço que os recebe. O Amazon S3 criptografa seus dados no nível do objeto, pois os grava em discos em seus data centers e os descriptografa para você quando você os acessa.

O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como o nível base 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 são criptografados automaticamente sem custo adicional e sem impacto no desempenho.

Criptografia do lado do servidor Amazon S3

O AWS KMS é um serviço que combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves dimensionado para a nuvem. O Amazon S3 usa criptografia do lado do servidor com o AWS KMS (SSE-KMS) para criptografar seus dados de objeto S3. Além disso, quando o SSE-KMS é solicitado para o objeto, a soma de verificação S3 como parte dos metadados do objeto é armazenada em formato criptografado.

Se você usar chaves KMS, poderá usar o AWS KMS por meio do AWS Management Console ou da API do AWS KMS para fazer o seguinte:

- Crie, visualize, edite, monitore, habilite ou desabilite, gire e agende a exclusão de chaves KMS de forma centralizada.
- Defina as políticas que controlam como e por quem as chaves KMS podem ser usadas.
- Audite o uso deles para provar que estão sendo usados corretamente. A auditoria é suportada pela API do AWS KMS, mas não pelo AWS KMSAWS Management Console.

Quando você habilita a rotação automática de chaves para uma chave KMS, o AWS KMS gera novo material criptográfico para a chave KMS todo ano.

Para o caso de uso fornecido, você pode configurar a criptografia do lado do servidor com chaves AWS KMS (SSE-KMS) com rotação automática de chaves.

Pergunta 43

Uma empresa de TI está trabalhando no engajamento do cliente para criar uma ferramenta de análise de dados em tempo real para dados da Internet das Coisas (IoT). Os dados da IoT são canalizados para o

Amazon Kinesis Data Streams, que também atua como a fonte de um fluxo de entrega para o Amazon Kinesis Firehose. A equipe de engenharia agora configurou um Kinesis Agent para enviar dados da IoT de outro conjunto de dispositivos para o mesmo fluxo de entrega do Amazon Kinesis Firehose. Eles notaram que os dados não estão chegando ao Kinesis Firehose como esperado. Como arquiteto de soluções, qual das seguintes opções você atribuiria como a causa raiz MAIS plausível por trás desse problema?

R: O Kinesis Agent não pode gravar no Amazon Kinesis Firehose para o qual a origem do fluxo de entrega já está definida como Amazon Kinesis Data Streams

Opção correta:

O Kinesis Agent não pode gravar no Amazon Kinesis Firehose para o qual a origem do fluxo de entrega já está definida como Amazon Kinesis Data Streams

O Amazon Kinesis Data Firehose é a maneira mais fácil de carregar dados de streaming de forma confiável em data lakes, data stores e ferramentas de análise. É um serviço totalmente gerenciado que dimensiona automaticamente para corresponder à taxa de transferência dos seus dados e não requer administração contínua. Ele também pode agrupar, compactar, transformar e criptografar os dados antes de carregá-los, minimizando a quantidade de armazenamento usada no destino e aumentando a segurança. Quando um Amazon Kinesis Data Stream é configurado como a origem de um fluxo de entrega do Kinesis

Firehose, as operações do Firehose `PutRecord` e `PutRecordBatch` são desabilitadas e o Kinesis Agent não pode gravar no Kinesis Firehose Delivery Stream diretamente. Os dados precisam ser adicionados ao Amazon Kinesis Data Stream por meio dos Kinesis Data `Streams` `PutRecord` e `PutRecords` operações. Portanto, esta opção está correta.

Pergunta 44

Uma empresa de serviços financeiros implantou seu aplicativo principal em instâncias do Amazon EC2. Como o aplicativo manipula dados confidenciais do cliente, a equipe de segurança da empresa quer garantir que todos os certificados SSL/Transport Layer Security (TLS) de terceiros configurados em instâncias do Amazon EC2 por meio do AWS Certificate Manager (ACM) sejam renovados antes da data de expiração. A empresa contratou você como um AWS Certified Solutions Architect Associate para criar uma solução que notifique a equipe de segurança 30 dias antes da expiração do certificado. A solução deve exigir o mínimo de scripts e esforço de manutenção.

`O que você recomendaria?`

R: Aproveite a regra gerenciada do AWS Config para verificar se algum certificado SSL/TLS de terceiros importado para o ACM está marcado para expiração em 30 dias. Configure a regra para disparar uma notificação do Amazon SNS para a equipe de segurança se algum certificado expirar em 30 dias

Opção correta:

Aproveite a regra gerenciada do AWS Config para verificar se algum certificado SSL/TLS de terceiros importado para o ACM está marcado para expiração em 30 dias. Configure a regra para disparar uma notificação do Amazon SNS para a equipe de segurança se algum certificado expirar em 30 dias

O AWS Certificate Manager é um serviço que permite que você provisione, gerencie e implante facilmente certificados Secure Sockets Layer/Transport Layer Security (SSL/TLS) públicos e privados para uso com serviços da AWS e seus recursos internos conectados. Os certificados SSL/TLS são usados para proteger comunicações de rede e estabelecer a identidade de sites na Internet, bem como recursos em redes privadas.

O AWS Config fornece uma visão detalhada da configuração dos recursos da AWS na sua conta da AWS. Isso inclui como os recursos estão relacionados entre si e como eles foram configurados no passado para que você possa ver como as configurações e os relacionamentos mudam ao longo do tempo.

O AWS Config fornece regras gerenciadas pela AWS, que são regras predefinidas e personalizáveis que o AWS Config usa para avaliar se seus recursos da AWS estão em conformidade com as melhores práticas

comuns. Você pode aproveitar uma regra gerenciada pelo AWS Config para verificar se algum certificado do ACM em sua conta está marcado para expiração dentro do número especificado de dias. Os certificados fornecidos pelo ACM são renovados automaticamente. O ACM não renova automaticamente os certificados que você importa. A regra é NON_COMPLIANT se seus certificados estiverem prestes a expirar.

Você pode configurar o AWS Config para transmitir alterações de configuração e notificações para um tópico do Amazon SNS. Por exemplo, quando um recurso é atualizado, você pode receber uma notificação enviada para seu e-mail, para que possa visualizar as alterações. Você também pode ser notificado quando o AWS Config avaliar suas regras personalizadas ou gerenciadas em relação aos seus recursos.

Pergunta 45

Um engenheiro júnior de DevOps quer alterar a configuração padrão para o encerramento de volume do Amazon EBS. Por padrão, o volume raiz de uma instância do Amazon EC2 para uma AMI com suporte do EBS é excluído quando a instância é encerrada.

Qual opção abaixo ajuda a alterar esse comportamento padrão para garantir que o volume persista mesmo após o término da instância?

R: Defina o `DeleteOnTermination` atributo como falso

Opção correta:

Defina o `DeleteOnTermination` atributo como falso

Uma instância do Amazon EC2 pode ser iniciada a partir de uma AMI com suporte de armazenamento de instância ou de uma AMI com suporte do Amazon EBS. Instâncias que usam o Amazon EBS para o dispositivo raiz têm automaticamente um volume do Amazon EBS anexado. Por padrão, o volume raiz de uma AMI com suporte do Amazon EBS é excluído quando a instância é encerrada. O comportamento padrão pode ser alterado para garantir que o volume persista após o encerramento da instância. Para alterar o comportamento padrão, defina o atributo DeleteOnTermination como false usando um mapeamento de dispositivo de bloco.

Pergunta 46

Uma agência de previsão do tempo coleta métricas climáticas importantes em várias cidades dos EUA e envia esses dados na forma de pares de chave-valor para a Nuvem AWS com uma frequência de um minuto.

Como arquiteto de soluções, qual dos seguintes serviços da AWS você usaria para criar uma solução para processar e armazenar esses dados de forma confiável e com alta disponibilidade? (Selecione duas)

R: Amazon DynamoDB
R: AWS Lambda

Opções corretas:

AWS Lambda
Com o AWS Lambda, você pode executar código sem provisionar ou gerenciar servidores. Você paga apenas pelo tempo de computação que consome — não há cobrança quando seu código não está em execução. Você pode executar código para praticamente qualquer tipo de aplicativo ou serviço de backend — tudo com administração zero.

Amazon DynamoDB
O Amazon DynamoDB é um banco de dados de chave-valor e documento que oferece desempenho de milissegundos de um dígito em qualquer escala. É um banco de dados totalmente gerenciado, multirregional, multimestre e durável com segurança integrada, backup e restauração e cache na memória para aplicativos em escala de internet. O Amazon DynamoDB é um banco de dados NoSQL e é mais adequado para armazenar dados em pares de chave-valor.
O AWS Lambda pode ser combinado com o DynamoDB para processar e capturar os dados de valor-chave das fontes de IoT descritas no caso de uso. Então, ambas as opções estão corretas.

Pergunta 47

Um aplicativo HTTP é implantado em um Grupo de Dimensionamento Automático, é acessível a partir de um Balanceador de Carga de Aplicativo (ALB) que fornece terminação HTTPS e acessa um banco de dados PostgreSQL gerenciado pelo Amazon RDS.

Como você deve configurar os grupos de segurança? (Selecione três)

R: O grupo de segurança do Application Load Balancer deve ter uma regra de entrada de qualquer lugar na porta 443

R: O grupo de segurança do Amazon RDS deve ter uma regra de entrada do grupo de segurança das instâncias do Amazon EC2 no grupo de dimensionamento automático na porta 5432

R: O grupo de segurança das instâncias do Amazon EC2 deve ter uma regra de entrada do grupo de segurança do Application Load Balancer na porta 80

Opções corretas:

O grupo de segurança do Amazon RDS deve ter uma regra de entrada do grupo de segurança das instâncias do Amazon EC2 no grupo de dimensionamento automático na porta 5432

O grupo de segurança das instâncias do Amazon EC2 deve ter uma regra de entrada do grupo de segurança do Application Load Balancer na porta 80

O grupo de segurança do Application Load Balancer deve ter uma regra de entrada de qualquer lugar na porta 443

Um grupo de segurança atua como um firewall virtual que controla o tráfego para uma ou mais instâncias. Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança; caso contrário, usamos o grupo de segurança padrão. Você pode adicionar regras a cada grupo de segurança que permite tráfego de ou para suas instâncias associadas. Você pode modificar as regras para um grupo de segurança a qualquer momento; as novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança. Quando decidimos se permitimos que o tráfego alcance uma instância, avaliamos todas as regras de todos os grupos de segurança associados à instância.

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

Porta PostgreSQL = 5432 Porta HTTP = 80 Porta HTTPS = 443

O tráfego ocorre assim: O cliente envia uma solicitação HTTPS para o ALB na porta 443. Isso é controlado pela regra - "O grupo de segurança do Application Load Balancer deve ter uma regra de entrada de qualquer lugar na porta 443"

O Application Load Balancer então encaminha a solicitação para uma das instâncias do Amazon EC2. Isso é tratado pela regra - "O grupo de segurança das instâncias do Amazon EC2 deve ter uma regra de entrada do grupo de segurança do Application Load Balancer na porta 80"

A instância do Amazon EC2 acessa ainda o banco de dados PostgreSQL gerenciado pelo Amazon RDS na porta 5432. Isso é controlado pela regra - "O grupo de segurança do Amazon RDS deve ter uma regra de entrada do grupo de segurança das instâncias do Amazon EC2 no grupo de dimensionamento automático na porta 5432"

Pergunta 48

Você foi contratado como Solutions Architect para aconselhar uma empresa sobre os vários mecanismos de autenticação/autorização que a AWS oferece para autorizar uma chamada de API dentro do Amazon API Gateway. A empresa prefere uma solução que ofereça gerenciamento de usuário integrado.

Qual das seguintes soluções você sugeriria como a mais adequada para o caso de uso em questão?

R: Use pools de usuários do Amazon Cognito

Opção correta:

Use pools de usuários do Amazon Cognito

Um pool de usuários é um diretório de usuários no Amazon Cognito. Você pode aproveitar os pools de usuários do Amazon Cognito para fornecer gerenciamento de usuários integrado ou integrar com provedores de identidade externos, como Facebook, Twitter, Google+ e Amazon. Não importa se seus usuários fazem login diretamente ou por meio de terceiros, todos os membros do pool de usuários têm um perfil de diretório que você pode acessar por meio de um Software Development Kit (SDK).

Os pools de usuários fornecem: 1. Serviços de inscrição e login. 2. Uma interface de usuário da Web integrada e personalizável para fazer login de usuários. 3. Login social com Facebook, Google, Login com Amazon e Login com Apple, bem como login com provedores de identidade SAML do seu pool de usuários. 4. Gerenciamento de diretório de usuários e perfis de usuários. 5. Recursos de segurança, como autenticação multifator (MFA), verificações de credenciais comprometidas, proteção contra aquisição de conta e verificação de telefone e e-mail. 6. Fluxos de trabalho personalizados e migração de usuários por meio de gatilhos do AWS Lambda.

Depois de criar um pool de usuários do Amazon Cognito, no API Gateway, você deve criar um autorizador COGNITO_USER_POOLS que use o pool de usuários.

Pergunta 49

Sua empresa tem uma carga de trabalho mensal de big data, em execução por cerca de 2 horas, que pode ser distribuída eficientemente em vários servidores de vários tamanhos, com um número variável de CPUs. A solução para a carga de trabalho deve ser capaz de suportar falhas de servidor.

Qual é a solução com melhor custo-benefício para essa carga de trabalho?

R: Execute a carga de trabalho em uma frota Spot

Opção correta:

Execute a carga de trabalho em uma frota Spot

O Spot Fleet seleciona os pools de Spot Instance que atendem às suas necessidades e inicia Spot Instances para atender à capacidade alvo para a frota. Por padrão, Spot Fleets são definidos para manter a capacidade alvo iniciando instâncias de substituição após Spot Instances na frota serem encerradas.

Uma Spot Instance é uma instância Amazon EC2 não utilizada que está disponível por menos do que o preço On-Demand. Spot Instances fornecem grande eficiência de custo, mas precisamos selecionar um tipo de instância com antecedência. Neste caso, queremos usar a opção mais econômica e deixar a seleção da instância spot mais barata para uma solicitação Spot Fleet, que pode ser otimizada com a `lowestPrice` estratégia. Então esta é a opção correta.

Pergunta 50

Uma startup acaba de desenvolver um serviço de backup de vídeo hospedado em uma frota de instâncias do Amazon EC2. As instâncias do Amazon EC2 estão por trás de um Application Load Balancer e as instâncias estão usando Amazon Elastic Block Store (Amazon EBS) Volumes para armazenamento. O serviço fornece aos usuários autenticados a capacidade de carregar vídeos que são salvos no volume EBS anexado a uma determinada instância. No primeiro dia do lançamento beta, os usuários começam a reclamar que conseguem ver apenas alguns dos vídeos em seu backup de vídeos carregados. Toda vez que os usuários fazem login no site, eles afirmam ver um subconjunto diferente de seus vídeos carregados.

Qual das seguintes opções é a solução MAIS otimizada para garantir que os usuários possam visualizar todos os vídeos enviados? (Selecione duas)

R: Escreva um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon S3 e, em seguida, modifique o aplicativo para usar o padrão Amazon S3 para armazenar os vídeos

R: Monte o Amazon Elastic File System (Amazon EFS) em todas as instâncias do Amazon EC2. Grave um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon EFS. Modifique o aplicativo para usar o Amazon EFS para armazenar os vídeos

Opções corretas:

Escreva um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon S3 e, em seguida, modifique o aplicativo para usar o padrão Amazon S3 para armazenar os vídeos

Monte o Amazon Elastic File System (Amazon EFS) em todas as instâncias do Amazon EC2. Grave um trabalho único para copiar os vídeos de todos os volumes do Amazon EBS para o Amazon EFS. Modifique o aplicativo para usar o Amazon EFS para armazenar os vídeos

- O Amazon Elastic Block Store (EBS) é um serviço de armazenamento em bloco de alto desempenho e fácil de usar, projetado para uso com o Amazon Elastic Compute Cloud (EC2) para cargas de trabalho com alto rendimento e transações em qualquer escala.

O Amazon Elastic File System (Amazon EFS) fornece um sistema de arquivos NFS elástico, simples, escalável e totalmente gerenciado para uso com serviços da AWS Cloud e recursos locais. Ele foi criado para escalar sob demanda para petabytes sem interromper os aplicativos, aumentando e diminuindo automaticamente conforme você adiciona e remove arquivos, eliminando a necessidade de provisionar e gerenciar capacidade para acomodar o crescimento.

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.

Como os volumes do Amazon EBS são anexados localmente às instâncias do Amazon EC2, portanto, os vídeos enviados são vinculados a instâncias específicas do Amazon EC2. Toda vez que o usuário faz login, ele é direcionado para uma instância diferente e, portanto, seus vídeos são dispersos em vários volumes do EBS. A solução correta é usar o Amazon S3 ou o Amazon EFS para armazenar os vídeos do usuário.

Pergunta 51

Uma empresa está desenvolvendo um aplicativo global de assistência médica que requer a menor latência possível para operações de leitura/gravação de banco de dados de usuários em várias regiões geográficas do mundo. A empresa contratou você como um AWS Certified Solutions Architect Associate para criar uma solução usando o Amazon Aurora que oferece um objetivo de ponto de recuperação (RPO) efetivo de segundos e um objetivo de tempo de recuperação (RTO) de um minuto.

Qual das seguintes opções você recomendaria?

R: Configurar um cluster do Amazon Aurora Global Database

Opção correta:

Configurar um cluster do Amazon Aurora Global Database

O Amazon Aurora Global Database foi projetado para aplicativos distribuídos globalmente, permitindo que um único banco de dados Amazon Aurora abranja várias regiões da AWS. Ele replica seus dados sem impacto no desempenho do banco de dados, permite leituras locais rápidas com baixa latência em cada região e fornece recuperação de desastres de interrupções em toda a região.

Se sua Região primária sofrer uma degradação de desempenho ou interrupção, você pode promover uma das Regiões secundárias para assumir responsabilidades de leitura/gravação. Um cluster Aurora pode se recuperar em menos de 1 minuto, mesmo no caso de uma interrupção regional completa. Isso fornece ao seu aplicativo um objetivo de ponto de recuperação (RPO) efetivo de 1 segundo e um objetivo de tempo de recuperação (RTO) de menos de 1 minuto, fornecendo uma base sólida para um plano global de continuidade de negócios.

Pergunta 52

Uma empresa de mídia está migrando seu aplicativo principal de seu data center local para a AWS para melhorar a capacidade de dimensionamento de leitura do aplicativo, bem como sua disponibilidade. A arquitetura existente aproveita um banco de dados Microsoft SQL Server que vê uma carga de leitura

pesada. A equipe de engenharia faz uma cópia completa do banco de dados de produção no início do dia útil para preencher um banco de dados dev. Durante esse período, os usuários do aplicativo enfrentam alta latência, o que leva a uma experiência ruim para o usuário.

A empresa está analisando opções alternativas de banco de dados e migrando mecanismos de banco de dados, se necessário. O que você sugere?

R: Aproveite o Amazon Aurora MySQL com réplicas Multi-AZ Aurora e crie o banco de dados dev restaurando a partir dos backups automatizados do Amazon Aurora

Opção correta:

Aproveite o Amazon Aurora MySQL com réplicas Multi-AZ Aurora e crie o banco de dados dev restaurando a partir dos backups automatizados do Amazon Aurora

O Amazon Aurora (Aurora) é um mecanismo de banco de dados relacional totalmente gerenciado que é compatível com MySQL e PostgreSQL. Um cluster de banco de dados do Amazon Aurora consiste em uma ou mais instâncias de banco de dados e um volume de cluster que gerencia os dados para essas instâncias de banco de dados. Um volume de cluster do Aurora é um volume de armazenamento de banco de dados virtual que abrange várias Zonas de Disponibilidade (AZs), com cada Zona de Disponibilidade (AZ) tendo uma cópia dos dados do cluster de banco de dados do Amazon Aurora. O Aurora oferece suporte a réplicas do Aurora Multi-AZ que melhoram o dimensionamento de leitura e a disponibilidade do aplicativo.

O Aurora faz backup do seu volume de cluster automaticamente e retém os dados de restauração durante o período de retenção do backup. Os backups do Aurora são contínuos e incrementais para que você possa restaurar rapidamente para qualquer ponto dentro do período de retenção do backup. Nenhum impacto no desempenho ou interrupção do serviço do banco de dados ocorre enquanto os dados de backup estão sendo gravados.

Os backups automatizados ocorrem diariamente durante a janela de backup preferencial. Se o backup exigir mais tempo do que o alocado para a janela de backup, o backup continuará após o término da janela, até que ela termine. A janela de backup não pode se sobrepor à janela de manutenção semanal para o cluster de BD. Os backups do Aurora são contínuos e incrementais, mas a janela de backup é usada para criar um backup diário do sistema que é preservado dentro do período de retenção de backup. O último tempo restaurável para um cluster de BD é o ponto mais recente no qual você pode restaurar seu cluster de BD, normalmente dentro de 5 minutos do horário atual.

Para o caso de uso fornecido, você pode criar o banco de dados dev restaurando a partir dos backups automatizados do Amazon Aurora.

Pergunta 53

Uma empresa de mídia criou uma conexão AWS Direct Connect para migrar seu aplicativo principal para a Nuvem AWS. O aplicativo local grava centenas de arquivos de vídeo em um sistema de arquivos NFS montado diariamente. Após a migração, a empresa hospedará o aplicativo em uma instância do Amazon EC2 com um sistema de arquivos Amazon Elastic File System (Amazon EFS) montado. Antes do corte da migração, a empresa deve criar um processo que replicará os arquivos de vídeo locais recém-criados para o sistema de arquivos Amazon EFS.

Qual das opções a seguir representa a maneira operacional MAIS eficiente de atender a esse requisito?

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

Opção correta:

Configure um agente AWS DataSync no servidor local que tenha acesso ao sistema de arquivos NFS. Transfira dados pela conexão AWS Direct Connect para um endpoint VPC da interface AWS PrivateLink para

Amazon EFS usando um VIF privado. Configure uma tarefa agendada do AWS DataSync para enviar os arquivos de vídeo para o sistema de arquivos Amazon EFS a cada 24 horas
O AWS DataSync é um serviço de transferência de dados online que simplifica, automatiza e acelera a cópia de grandes quantidades de dados entre sistemas de armazenamento locais e serviços de armazenamento da AWS, bem como entre serviços de armazenamento da AWS.
Você pode usar o AWS DataSync para migrar dados localizados no local, na borda ou em outras nuvens para o Amazon S3, Amazon EFS, Amazon FSx para Windows File Server, Amazon FSx para Lustre, Amazon FSx para OpenZFS e Amazon FSx para NetApp ONTAP.

Para estabelecer uma conexão privada entre sua nuvem privada virtual (VPC) e a API do Amazon EFS, você pode criar um endpoint de VPC de interface. Você também pode acessar o endpoint de VPC de interface de ambientes locais ou outros VPCs usando AWS VPN, AWS Direct Connect ou peering de VPC.
O AWS Direct Connect fornece três tipos de interfaces virtuais: pública, privada e de trânsito.

Para o caso de uso fornecido, você pode enviar dados pela conexão Direct Connect para um endpoint VPC da interface AWS PrivateLink para Amazon EFS usando um VIF privado.

Usando o agendamento de tarefas no AWS DataSync, você pode executar periodicamente uma tarefa de transferência do seu sistema de armazenamento de origem para o destino. Você pode usar a tarefa agendada do DataSync para enviar os arquivos de vídeo para o sistema de arquivos Amazon EFS a cada 24 horas.

Pergunta 54

Você gostaria de migrar uma conta da AWS de uma Organização A da AWS para uma Organização B da AWS. Quais são as etapas para isso?

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

Opção correta:

Remova a conta de membro da organização antiga. Envie um convite para a conta de membro da nova organização. Aceite o convite para a nova organização da conta de membro
O AWS Organizations ajuda você a governar centralmente seu ambiente conforme você cresce e dimensiona suas cargas de trabalho na AWS. Usando o AWS Organizations, você pode automatizar a criação de contas, criar grupos de contas para refletir suas necessidades comerciais e aplicar políticas para esses grupos para governança. Você também pode simplificar o faturamento configurando um único método de pagamento para todas as suas contas da AWS. Por meio de integrações com outros serviços da AWS, você pode usar o Organizations para definir configurações centrais e compartilhamento de recursos entre contas em sua organização.
Para migrar contas de uma organização para outra, você deve ter acesso root ou IAM às contas de membro e mestre. Aqui estão as etapas a seguir: 1. Remova a conta de membro da organização antiga 2. Envie um convite para a conta de membro da nova organização 3. Aceite o convite para a nova organização da conta de membro

Pergunta 55

Uma empresa de varejo quer lançar e testar uma implantação azul-verde para seu aplicativo global nas próximas 48 horas. A maioria dos clientes usa telefones celulares que são propensos ao cache do Sistema de Nomes de Domínio (DNS). A empresa tem apenas dois dias para a venda anual de Ação de Graças começar.

Como arquiteto de soluções, qual das seguintes opções você recomendaria para testar a implantação no maior número possível de usuários no período determinado?

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

Opção correta:

A implantação azul/verde é uma técnica para liberar aplicativos transferindo o tráfego entre dois ambientes idênticos que executam versões diferentes do aplicativo: "Azul" é a versão em execução e "verde" a nova versão. Esse tipo de implantação permite testar recursos no ambiente verde sem afetar a versão em execução do aplicativo. Quando estiver satisfeito com o funcionamento correto da versão verde, você poderá redirecionar gradualmente o tráfego do antigo ambiente azul para o novo ambiente verde. As implantações azul/verde podem mitigar riscos comuns associados à implantação de software, como tempo de inatividade e capacidade de reversão.

Use o AWS Global Accelerator para distribuir uma parte do tráfego para uma implantação específica
O AWS Global Accelerator é um serviço de camada de rede que direciona o tráfego para endpoints ideais na rede global da AWS, o que melhora a disponibilidade e o desempenho dos seus aplicativos de internet. Ele fornece dois endereços IP anycast estáticos que atuam como um ponto de entrada fixo para os endpoints do seu aplicativo em uma ou várias regiões da AWS, como seus Application Load Balancers, Network Load Balancers, endereços Elastic IP ou instâncias do Amazon EC2, em uma ou várias regiões da AWS.
O AWS Global Accelerator usa pesos de endpoint para determinar a proporção de tráfego que é direcionado para endpoints em um grupo de endpoints e mostradores de tráfego para controlar a porcentagem de tráfego que é direcionado para um grupo de endpoints (uma região da AWS onde seu aplicativo é implantado).
Embora confiar no serviço DNS seja uma ótima opção para implantações azuis/verdes, ele pode não se adequar a casos de uso que exigem uma transição rápida e controlada do tráfego. Alguns dispositivos clientes e resolvedores de internet armazenam em cache respostas DNS por longos períodos; esse recurso DNS melhora a eficiência do serviço DNS, pois reduz o tráfego DNS pela Internet e serve como uma técnica de resiliência, evitando sobrecargas de servidores de nomes autoritativos. A desvantagem disso em implantações azuis/verdes é que você não sabe quanto tempo levará para que todos os seus usuários recebam endereços IP atualizados quando você atualiza um registro, altera sua preferência de roteamento ou quando há uma falha no aplicativo.
Com o AWS Global Accelerator, você pode transferir o tráfego gradualmente ou de uma só vez entre o ambiente azul e o verde e vice-versa sem estar sujeito ao cache de DNS em dispositivos clientes e resolvedores de internet, as marcações de tráfego e as alterações de pesos de endpoint entram em vigor em segundos.

Pergunta 56

Considere a seguinte política associada a um grupo IAM contendo vários usuários:

```
{
    "Version":"2012-10-17",
    "Id":"EC2TerminationPolicy",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":"ec2:*",
            "Resource":"*",
            "Condition":{
                "StringNotEquals":{
                    "ec2:Region":"us-west-1"
                }
            }
        },
        {
            "Effect":"Allow",
            "Action":"ec2:TerminateInstances",
            "Resource":"*",
            "Condition":{
                "IpAddress":{
                    "aws:SourceIp":"10.200.200.0/24"
                }
            }
        }
    ]
}
```

Qual das seguintes opções está correta?

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

Opção correta:

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

A política fornecida nega todas as ações de especificação do EC2 em todos os recursos quando a região do recurso subjacente não é `us-west-1` . A política permite a ação terminate EC2 em todos os recursos quando o endereço IP de origem está no intervalo CIDR 10.200.200.0/24, portanto, permitiria que o
usuário com o IP de origem 10.200.200.200 encerrasse a instância do Amazon EC2.

Pergunta 57

Um aplicativo de mídia social é hospedado em uma frota Amazon EC2 em execução atrás de um Application Load Balancer. O tráfego do aplicativo é fronteado por uma distribuição Amazon CloudFront. A equipe de engenharia quer desacoplar o processo de autenticação do usuário para o aplicativo, para que os servidores de aplicativo possam se concentrar apenas na lógica de negócios.

Como arquiteto de soluções, qual das seguintes soluções você recomendaria à equipe de desenvolvimento para que exija o mínimo de esforço de desenvolvimento?

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

Opção correta:

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

O Application Load Balancer pode ser usado para autenticar usuários com segurança para acessar seus aplicativos. Isso permite que você transfira o trabalho de autenticação de usuários para o seu balanceador de carga, permitindo que seus aplicativos se concentrem em sua lógica de negócios. Você pode usar os Cognito User Pools para autenticar usuários por meio de IdPs sociais conhecidos, como Amazon, Facebook ou Google, por meio dos pools de usuários suportados pelo Amazon Cognito, ou por meio de identidades corporativas, usando SAML, LDAP ou Microsoft AD, por meio dos pools de usuários suportados pelo Amazon Cognito. Você configura a autenticação de usuários criando uma ação de autenticação para uma ou mais regras de ouvinte.

Alerta de exame:

Revise a nota a seguir para entender as diferenças entre os pools de usuários do Amazon Cognito e os pools de identidades do Amazon Cognito.

Pergunta 58

Uma empresa de segurança cibernética usa uma frota de instâncias do Amazon EC2 para executar um aplicativo proprietário. O grupo de manutenção de infraestrutura da empresa quer ser notificado por e-mail sempre que a utilização da CPU para qualquer uma das instâncias do Amazon EC2 violar um determinado limite.

Qual dos seguintes serviços você usaria para construir uma solução com MENOR esforço de desenvolvimento? (Selecione dois)

R: Amazon CloudWatch
R: Serviço de notificação simples da Amazon (Amazon SNS)

Opções corretas:

Serviço de notificação simples da Amazon (Amazon SNS)

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

Amazon CloudWatch

O Amazon CloudWatch é um serviço de monitoramento e observabilidade criado para engenheiros de DevOps, desenvolvedores, engenheiros de confiabilidade de site (SREs) e gerentes de TI. O Amazon CloudWatch fornece dados e insights acionáveis para monitorar seus aplicativos, responder a mudanças de desempenho em todo o sistema, otimizar a utilização de recursos e obter uma visão unificada da saúde operacional. O Amazon CloudWatch permite que você monitore os recursos de nuvem da AWS e os aplicativos que você executa na AWS.

Você pode usar o Amazon CloudWatch Alarms para enviar um e-mail via Amazon SNS sempre que qualquer uma das instâncias do Amazon EC2 violar um certo limite. Portanto, ambas as opções estão corretas.

Pergunta 59

Um desenvolvedor precisa implementar uma função do AWS Lambda na conta A da AWS que acessa um bucket do Amazon Simple Storage Service (Amazon S3) na conta B da AWS.

Como arquiteto de soluções, qual das opções a seguir você recomendaria para atender a esse requisito?

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

Opção correta:

Crie uma função do IAM para a função do AWS Lambda que conceda acesso ao bucket do Amazon S3. Defina a função do IAM como a função de execução da função do AWS Lambda. Certifique-se de que a política do bucket também conceda acesso à função de execução da função do AWS Lambda
Se a função do IAM que você criar para a função do Lambda estiver na mesma conta da AWS que o bucket, não será necessário conceder permissões do Amazon S3 na função do IAM e na política do bucket. Em vez disso, você pode conceder as permissões na função do IAM e, em seguida, verificar se a política do bucket não nega explicitamente o acesso à função do Lambda. Se a função do IAM e o bucket estiverem em contas diferentes, será necessário conceder permissões do Amazon S3 na função do IAM e na política do bucket. Portanto, esta é a maneira correta de dar acesso ao AWS Lambda para o caso de uso fornecido.

Pergunta 60

Você tem uma equipe de desenvolvedores em sua empresa e gostaria de garantir que eles possam experimentar rapidamente as AWS Managed Policies anexando-as às suas contas, mas gostaria de impedi- los de fazer uma escalada de privilégios, concedendo a si mesmos a AdministratorAccessmanaged policy. Como você deve proceder?
Para cada desenvolvedor, defina um limite de permissão do IAM que restringirá as políticas gerenciadas que eles podem anexar a si mesmos

Opção correta:

Para cada desenvolvedor, defina um limite de permissão do IAM que restringirá as políticas gerenciadas que eles podem anexar a si mesmos
A AWS oferece suporte a limites de permissões para entidades do IAM (usuários ou funções). Um limite de permissões é um recurso avançado para usar uma política gerenciada para definir as permissões máximas que uma política baseada em identidade pode conceder a uma entidade do IAM. O limite de permissões de uma entidade permite que ela execute apenas as ações permitidas por suas políticas baseadas em identidade e seus limites de permissões. Aqui, temos que usar um limite de permissão do IAM. Eles só podem ser aplicados a funções ou usuários, não a grupos do IAM.

Pergunta 61

Você tem várias contas da AWS em uma única região da AWS gerenciada por organizações da AWS e gostaria de garantir que todas as instâncias do Amazon EC2 em todas essas contas possam se comunicar de forma privada. Qual das seguintes soluções fornece a capacidade pelo custo MAIS BARATO?
R: Crie uma nuvem privada virtual (VPC) em uma conta e compartilhe uma ou mais de suas sub-redes com as outras contas usando o Resource Access Manager

Opção correta:

Crie uma nuvem privada virtual (VPC) em uma conta e compartilhe uma ou mais de suas sub-redes com as outras contas usando o Resource Access Manager

O AWS Resource Access Manager (RAM) é um serviço que permite que você compartilhe recursos da AWS de forma fácil e segura com qualquer conta da AWS ou dentro da sua organização da AWS. Você pode compartilhar recursos de AWS Transit Gateways, sub-redes, configurações do AWS License Manager e regras do Amazon Route 53 Resolver com o RAM. O RAM elimina a necessidade de criar recursos duplicados em várias contas, reduzindo a sobrecarga operacional de gerenciar esses recursos em cada conta que você possui. Você pode criar recursos centralmente em um ambiente de várias contas e usar o RAM para compartilhar esses recursos entre contas em três etapas simples: criar um Resource Share, especificar recursos e especificar contas. O RAM está disponível para você sem custo adicional.
A solução correta é compartilhar a(s) sub-rede(s) dentro de uma VPC usando RAM. Isso permitirá que todas as instâncias do Amazon EC2 sejam implantadas na mesma VPC (embora de contas diferentes) e se comuniquem facilmente entre si.

Pergunta 62

Sua empresa tem um serviço de replicação de sistema de arquivos distribuído (DFSR) local para manter arquivos sincronizados em vários servidores Windows e gostaria de migrar para a nuvem AWS.

O que você recomenda como substituto para o DFSR?

R: Amazon FSx para servidor de arquivos do Windows

Opção correta:

Amazon FSx para servidor de arquivos do Windows

O Amazon FSx para Windows File Server fornece armazenamento de arquivos totalmente gerenciado e altamente confiável que é acessível pelo protocolo Service Message Block (SMB) padrão do setor. Ele é criado no Windows Server, fornecendo uma ampla gama de recursos administrativos, como cotas de usuário, restauração de arquivo de usuário final e integração com o Microsoft Active Directory (AD). O serviço Distributed File System Replication (DFSR) é um novo mecanismo de replicação multimestre usado para manter pastas sincronizadas em vários servidores. O Amazon FSx oferece suporte ao uso do Distributed File System (DFS) da Microsoft para organizar compartilhamentos em uma única estrutura de pastas de até centenas de PB de tamanho.
O Amazon FSx para Windows é um sistema de arquivos distribuído perfeito, com capacidade de replicação, e pode ser montado no Windows.

Pergunta 63

Uma startup baseada no Vale do Silício tem uma arquitetura de duas camadas usando instâncias do Amazon EC2 para seu aplicativo principal. Os servidores web (escutando na porta 443), que foram atribuídos ao grupo de segurança A, estão em sub-redes públicas em duas Zonas de Disponibilidade (AZs) e as instâncias de banco de dados baseadas em MSSQL (escutando na porta 1433), que foram atribuídas ao grupo de segurança B, estão em duas sub-redes privadas em duas Zonas de Disponibilidade (AZs). A equipe de DevOps quer revisar as configurações de segurança da arquitetura do aplicativo.

Como arquiteto de soluções, qual das seguintes opções você selecionaria como a configuração MAIS segura? (Selecione duas)

R: Para o grupo de segurança B: adicione uma regra de entrada que permita tráfego somente do grupo de segurança A na porta 1433

R: Para o grupo de segurança A: adicione uma regra de entrada que permita tráfego de todas as origens na porta 443. Adicione uma regra de saída com o destino como grupo de segurança B na porta 1433

Opções corretas:
Para o grupo de segurança A: adicione uma regra de entrada que permita tráfego de todas as origens na porta 443. Adicione uma regra de saída com o destino como grupo de segurança B na porta 1433

Para o grupo de segurança B: adicione uma regra de entrada que permita tráfego somente do grupo de segurança A na porta 1433

Um grupo de segurança atua como um firewall virtual que controla o tráfego para uma ou mais instâncias. Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança; caso contrário, usamos o grupo de segurança padrão. Você pode adicionar regras a cada grupo de segurança que permite tráfego de ou para suas instâncias associadas. Você pode modificar as regras para um grupo de segurança a qualquer momento; as novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança. Quando decidimos se permitimos que o tráfego alcance uma instância, avaliamos todas as regras de todos os grupos de segurança associados à instância.
A seguir estão as características das regras do grupo de segurança:
Por padrão, os grupos de segurança permitem todo o tráfego de saída.
As regras do grupo de segurança são sempre permissivas; você não pode criar regras que neguem acesso.
Os grupos de segurança são estatais
A configuração MAIS segura para o caso de uso fornecido é:
Para o grupo de segurança A: adicione uma regra de entrada que permita tráfego de todas as origens na porta 443. Adicione uma regra de saída com o destino como grupo de segurança B na porta 1433
As regras acima garantem que os servidores web estejam escutando o tráfego em todas as fontes no protocolo HTTPS na porta 443. Os servidores web só permitem tráfego de saída para servidores MSSQL no Grupo de Segurança B na porta 1433.
Para o grupo de segurança B: adicione uma regra de entrada que permita tráfego somente do grupo de segurança A na porta 1433. A regra acima garante que os servidores MSSQL aceitem somente tráfego de servidores web no grupo de segurança A na porta 1433.
Portanto, ambas as opções estão corretas.

Pergunta 64

Uma empresa de serviços financeiros quer um único modelo de processamento de log para todos os arquivos de log (consistindo em logs de sistema, logs de aplicativo, logs de banco de dados, etc.) que podem ser processados de forma serverless e então armazenados de forma durável para análise downstream. A empresa quer usar um serviço gerenciado da AWS que dimensiona automaticamente para corresponder à taxa de transferência dos dados de log e não requer administração contínua.

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

R: Amazon Kinesis Data Firehose

Opção correta:

Amazon Kinesis Data Firehose
O Amazon Kinesis Data Firehose é a maneira mais fácil de carregar dados de streaming de forma confiável em data lakes, data stores e ferramentas de análise. Ele pode capturar, transformar e carregar dados de streaming no Amazon S3, Amazon Redshift, Amazon Elasticsearch Service e Splunk, permitindo análises quase em tempo real com ferramentas de inteligência empresarial e painéis existentes que você já usa hoje. É um serviço totalmente gerenciado que dimensiona automaticamente para corresponder à taxa de transferência dos seus dados e não requer administração contínua. Portanto, esta é a opção correta.

Pergunta 65

O que esta política de IAM faz?

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "34.50.31.0/24"
        }
      }
    }
  ]
}
```

R: Ele permite iniciar uma instância do Amazon EC2 somente quando o IP de onde a chamada se origina está dentro do `34.50.31.0/24` bloco CIDR

Opção correta:

Ele permite iniciar uma instância do Amazon EC2 somente quando o IP de onde a chamada se origina está dentro do `34.50.31.0/24` bloco CIDR

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "34.50.31.0/24"
        }
```

```
      }
    }
  ]
}
```

O `aws:SourceIP` nesta condição sempre representa o IP do chamador da API. Isso é muito útil se você quiser restringir o acesso a determinada API da AWS, por exemplo, do IP público da sua infraestrutura local.

Veja esta visão geral de endereços IP elásticos, públicos e privados:

Endereço IP elástico (EIP) - Um endereço IP elástico (EIP) 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 em sua conta.

Endereço IP privado - Um endereço IPv4 privado é um endereço IP que não pode ser acessado pela Internet. Você pode usar endereços IPv4 privados para comunicação entre instâncias na mesma VPC.

Endereço IP público - Um endereço IP público é um endereço IPv4 que pode ser acessado pela Internet. Você pode usar endereços públicos para comunicação entre suas instâncias e a Internet.

Observe `34.50.31.0/24` que é um intervalo de IP público, não um intervalo de IP privado. Os intervalos de IP privados são: 192.168.0.0 - 192.168.255.255 (65.536 endereços de IP) 172.16.0.0 - 172.31.255.255

(1.048.576 endereços de IP) 10.0.0.0 - 10.255.255.255 (16.777.216 endereços de IP)