

1. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma agência governamental planeja armazenar documentos fiscais confidenciais na AWS. Devido às informações confidenciais contidas nos arquivos, o Arquiteto de Soluções deve restringir as solicitações de acesso a dados feitas à solução de armazenamento a uma VPC específica da Amazon. A solução também deve impedir que os arquivos sejam excluídos ou substituídos para atender ao requisito regulatório de ter um modelo de armazenamento WORM (gravação única, leitura múltipla). Qual combinação das seguintes opções o Arquiteto deve implementar? (Selecione DUAS.)

Crie um novo bucket do Amazon S3 com o recurso Bloqueio de Objetos do S3 habilitado. Armazene os documentos no bucket e defina a opção "Retenção Legal" para retenção de objetos.

Configure um ponto de acesso do Amazon S3 para o bucket S3 para restringir o acesso aos dados somente a uma VPC específica.

Os pontos de acesso do Amazon S3 simplificam o acesso a dados para qualquer serviço da AWS ou aplicativo de cliente que armazene dados no S3. Os pontos de acesso são endpoints de rede nomeados que são anexados a buckets que você pode usar para executar operações de objetos do S3, como `GetObject` e `PutObject`.

Cada ponto de acesso possui permissões e controles de rede distintos que o S3 aplica a qualquer solicitação feita por meio dele. Cada ponto de acesso aplica uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Você pode configurar qualquer ponto de acesso para aceitar solicitações apenas de uma nuvem privada virtual (VPC) para restringir o acesso aos dados do Amazon S3 a uma rede privada. Você também pode definir configurações personalizadas de bloqueio de acesso público para cada ponto de acesso.

The screenshot shows the AWS S3 Access Points configuration interface. On the left sidebar, under the 'Access Points' section, there is a list of options: Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, Access analyzer for S3, Block Public Access settings for this account, Storage Lens (expanded), Dashboards, AWS Organizations settings, Feature spotlight (with 3 notifications), and AWS Marketplace for S3.

The main panel displays the 'Properties' for a new access point named 'tutorialsdojo-manila-s3-access-point'. The 'Bucket name' field is set to 'tutorialsdojo'. The 'AWS Region' is set to 'Asia Pacific (Sydney) ap-southeast-2'. Under 'Network origin', the 'Virtual private cloud (VPC)' option is selected, with a note explaining that the S3 console doesn't support VPC access points. The 'VPC ID' field contains 'vpc-0612abacada1898'. A blue callout bubble highlights this VPC ID field with the text: 'Specific Amazon VPC ID that has exclusive access to the S3 bucket'. The 'Block Public Access settings for this Access Point' section includes a checked checkbox for 'Block all public access'.

Você também pode usar os Pontos de Acesso Multirregionais do Amazon S3 para fornecer um endpoint global que os aplicativos podem usar para atender a solicitações de buckets do S3 localizados em várias regiões da AWS. Você pode usar os Pontos de Acesso Multirregionais para criar aplicativos multirregionais com a mesma arquitetura simples usada em uma única região e, em seguida, executar esses aplicativos em qualquer lugar do mundo. Em vez de enviar solicitações pela Internet pública congestionada, os Pontos de Acesso Multirregionais fornecem resiliência de rede integrada com aceleração de solicitações baseadas na Internet para o Amazon S3. As solicitações de aplicativos feitas a um endpoint global de Ponto de Acesso Multirregional usam o AWS Global Accelerator para rotear automaticamente pela rede global da AWS para o bucket do S3 com a menor latência de rede.

Com o S3 Object Lock, você pode armazenar objetos usando um modelo WORM (gravação única, leitura múltipla). O Object Lock pode ajudar a impedir que objetos sejam excluídos ou substituídos por um período fixo ou indefinidamente. Você pode usar o Object Lock para atender aos requisitos regulatórios que exigem armazenamento WORM ou simplesmente adicionar outra camada de proteção contra alterações e exclusões de objetos.

The screenshot shows the AWS S3 console with the 'Edit Object Lock' page open for a bucket named 'test-td-bucket'. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens (expanded to show Dashboards and Storage Lens groups), and AWS Organizations settings. The main content area displays the 'Edit Object Lock' section with a note that Object Lock works only on Versioned buckets, followed by 'Enable Versioning' and 'Diagnose with Amazon Q' buttons. Below this is the 'Object Lock' section, which contains a note about using a WORM model to prevent deletion or overwriting, and two radio button options: 'Disable' (selected) and 'Enable'. The 'Enable' option is described as permanently allowing objects to be locked. At the bottom right are 'Cancel' and 'Save changes' buttons. A 'Feature spotlight' badge with the number '7' is visible in the bottom-left corner of the sidebar.

Antes de bloquear qualquer objeto, é essencial habilitar o S3 Object Lock em um bucket. Anteriormente, o Object Lock só podia ser habilitado no momento da criação do bucket, mas agora, o Amazon S3 permite que você habilite o S3 Object Lock para buckets existentes com apenas alguns cliques. Uma vez que o S3 Object Lock é habilitado em um bucket, ele permite que você bloqueeie objetos dentro desse bucket para impedir que eles sejam excluídos ou substituídos por um período fixo ou indefinidamente. Embora o Object Lock agora possa ser habilitado em buckets existentes, é importante observar que, uma vez habilitado, o Object Lock em si não pode ser desabilitado. No entanto, você ainda pode gerenciar e configurar as definições de bloqueio de objetos, incluindo períodos de retenção e retenções legais, mas o recurso principal do Object Lock permanece ativo e irreversível. Além disso, o controle de versão, que é necessário para o Object Lock, não pode ser suspenso ou desabilitado depois que o Object Lock é habilitado no bucket.

Portanto, as respostas corretas são:

- Configure um ponto de acesso do Amazon S3 para o bucket S3 para restringir o acesso aos dados somente a uma VPC específica.

- Crie um novo bucket do Amazon S3 com o recurso Bloqueio de Objetos do S3 habilitado. Armazene os documentos no bucket e defina a opção Retenção Legal para retenção de objetos.

A opção que diz: **Configurar um novo bucket do Amazon S3 para armazenar os documentos fiscais e integrá-lo ao Firewall de Rede da AWS. Configurar o Firewall de Rede para aceitar apenas solicitações de acesso a dados de uma VPC específica** está incorreta, pois você não pode usar um Firewall de Rede da AWS diretamente para restringir as solicitações de acesso a dados do bucket do S3 a uma VPC específica da Amazon. Você precisa usar um Ponto de Acesso do Amazon S3 para este caso de uso específico. Um Firewall de Rede da AWS geralmente é integrado à sua VPC da Amazon e não a um bucket do S3.

A opção que diz: **Armazene os documentos fiscais na classe de armazenamento Amazon S3 Glacier Instant Retrieval. Usar a PutBucketPolicy API para aplicar uma política de bucket que restringe solicitações de acesso a uma VPC específica** está incorreta, pois o Amazon S3 Glacier Instant Retrieval é apenas uma classe de armazenamento de arquivamento que oferece o menor custo de armazenamento para dados de longa duração que raramente são acessados e exigem recuperação em milissegundos. Além disso, usar uma política de bucket para restringir o acesso de uma VPC é menos eficiente em comparação ao uso de um ponto de acesso S3.

A opção que diz: **Habilitar Bloqueio de Objetos, mas desabilitar o Controle de Versão de Objetos no novo bucket do Amazon S3 para atender ao requisito do modelo de armazenamento WORM (gravação única e leitura múltipla)** está incorreta. Embora o recurso Bloqueio de Objetos ofereça armazenamento WORM (gravação única e leitura múltipla), o recurso Controle de Versão de Objetos também precisa estar habilitado para que isso funcione. Aliás, você não pode desabilitar manualmente o recurso Controle de Versão de Objetos se já tiver selecionado a opção Bloqueio de Objetos.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

Justificativa:

A pergunta exige uma solução que:

- Restrinja o acesso ao armazenamento **somente a uma VPC específica**
- Impeça a exclusão ou modificação de dados (**modelo WORM**)
- Esteja **em conformidade com regulamentações governamentais** de proteção de dados

O S3 Object Lock (Bloqueio de Objetos):

- Permite armazenar objetos no modo **WORM**
- Suporta retenção por tempo definido e **retenção legal**, que impede modificações e exclusões
- Atende aos requisitos regulatórios de integridade e imutabilidade de dados

O S3 Access Point com restrição à VPC:

- Permite criar um endpoint dedicado para acesso ao bucket
- **Restringe o acesso ao bucket somente a uma VPC específica**, conforme exigido na questão
- Melhora o controle de acesso sem alterar a política global do bucket

Resumo Final:

A combinação do **S3 Object Lock** com **retenção legal** e um **S3 Access Point restrito à VPC** oferece uma solução segura, imutável e conforme os requisitos de regulamentação. Ela garante que os documentos fiscais confidenciais não sejam excluídos ou alterados e que apenas sistemas internos da VPC tenham acesso, atendendo integralmente aos critérios da agência governamental.

2. PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa hospedava um site de comércio eletrônico em um grupo de Auto Scaling de instâncias do Amazon EC2, atrás de um Application Load Balancer. O Arquiteto de Soluções notou que o site estava recebendo um alto número de solicitações externas ilegítimas de vários sistemas com endereços IP que mudavam com frequência. Para resolver os problemas de desempenho, o Arquiteto de Soluções precisa implementar uma solução que bloqueie essas solicitações, com impacto mínimo no tráfego legítimo. Qual das seguintes opções atende a esse requisito?

Crie uma regra baseada em taxa no AWS WAF e associe a ACL da Web a um Application Load Balancer.

O AWS WAF é totalmente integrado ao Amazon CloudFront, ao Application Load Balancer (ALB), ao Amazon API Gateway e ao AWS AppSync – serviços que os clientes da AWS costumam usar para fornecer conteúdo para seus sites e aplicativos. Ao usar o AWS WAF no Amazon CloudFront, suas regras são executadas em todos os AWS Edge Locations, localizados ao redor do mundo, próximos aos seus usuários finais. Isso significa que a segurança não compromete o desempenho. As solicitações bloqueadas são interrompidas antes de chegarem aos seus servidores web. Ao usar o AWS WAF em serviços regionais, como o Application Load Balancer, o Amazon API Gateway e o AWS AppSync, suas regras são executadas na região e podem ser usadas para proteger recursos da Internet, bem como recursos internos.

The screenshot shows the AWS WAF Rule builder interface. At the top, there are tabs for 'Rule visual editor' and 'Rule JSON editor'. A red arrow points to the 'Rate-based rule' option under the 'Type' section, which is highlighted with a yellow box. Below this, the 'Rate-limiting criteria' section is expanded, showing fields for 'Rate limit' (set to 100) and 'Evaluation window' (set to 5 minutes). The 'Request aggregation' section is also visible at the bottom.

Select 'Rate-based rule'

Rate limit
The maximum number of requests to allow during the specified time window that satisfy your criteria. You can narrow the scope of the requests using a scope-down statement. You can group requests by component types for count aggregation. You must provide at least one aggregation component or a scope-down statement.

100

Rate limit must be between 10 and 2,000,000,000.

Evaluation window
The amount of time to use for request counts.

5 minutes (300 seconds)

The default time span is 5 minutes. Valid values are 1, 2, 5, and 10 minutes.

Request aggregation

TUTORIALS DO JO

Uma regra baseada em taxa rastreia a taxa de solicitações para cada endereço IP de origem e aciona ação da regra em IPs com taxas que excedem um limite. Você define o limite como o número de solicitações por intervalo de 5 minutos. Você pode usar esse tipo de regra para bloquear temporariamente solicitações de um endereço IP que esteja enviando solicitações excessivas.

Com base no cenário apresentado, o requisito é limitar o número de solicitações ilegítimas sem afetar as solicitações genuínas. Para atender a esse requisito, você pode usar a ACL da Web do AWS WAF. Existem dois tipos de regras ao criar sua própria ACL da Web: regras regulares e regras baseadas em taxa. Você precisa selecionar a última para adicionar um limite de taxa à sua ACL da Web. Após criar a ACL da Web, você pode associá-la ao ALB. Quando a ação da regra for acionada, o AWS WAF aplicará a ação a solicitações adicionais do endereço IP até que a taxa de solicitações fique abaixo do limite.

Portanto, a resposta correta é: **Crie uma regra baseada em taxa no AWS WAF e associe a ACL da Web a um Application Load Balancer.**

A opção que diz: **Criar uma regra regular no AWS WAF e associar a ACL da Web a um Application Load Balancer** está incorreta porque uma regra regular normalmente corresponde à instrução definida na regra. Se precisar adicionar um limite de taxa à sua regra, crie uma regra baseada em taxa.

A opção que diz: **Criar uma ACL de rede personalizada e associá-la à sub-rede do Application Load Balancer para bloquear as solicitações ofensivas** está incorreta. Embora as NACLs possam ajudar a bloquear o tráfego de entrada, essa opção não seria capaz de limitar o número de solicitações de um único endereço IP que muda dinamicamente.

A opção que diz: **Criar uma regra personalizada no grupo de segurança do Application Load Balancer para bloquear as solicitações ofensivas** está incorreta porque o grupo de segurança só permite tráfego de entrada. Lembre-se de que você não pode negar tráfego usando grupos de segurança. Além disso, ele não é capaz de limitar a taxa de tráfego para sua aplicação, ao contrário do AWS WAF.

Referências:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

<https://aws.amazon.com/waf/faqs/>

Confira esta folha de dicas do AWS WAF:

<https://tutorialsdojo.com/aws-waf/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Bloqueie **requisições suspeitas e abusivas**
- **Minimize o impacto** em usuários legítimos
- Funcione com IPs **que mudam com frequência**
- Seja eficaz contra **picos de tráfego malicioso**

O AWS WAF com regras baseadas em taxa:

- **Monitora a taxa de requisições por IP** em tempo real
- Bloqueia **IPs que excedem limites configurados**
- Protege contra ataques de negação de serviço em nível de aplicação (Layer 7)
- É **altamente configurável e granular**, permitindo regras específicas
- Pode ser **associado diretamente ao ALB**, garantindo proteção integrada
- **Não afeta tráfego legítimo** se corretamente calibrado

Resumo Final:

O AWS WAF com regras baseadas em taxa é a solução **mais apropriada, eficiente e de baixo impacto** para bloquear requisições ilegítimas e proteger um site atrás de um ALB. Essa abordagem permite **detectar e mitigar abusos com IPs variáveis**, mantendo a **experiência dos usuários legítimos** e evitando degradação do desempenho, sem necessidade de infraestrutura adicional.

3. Pergunta

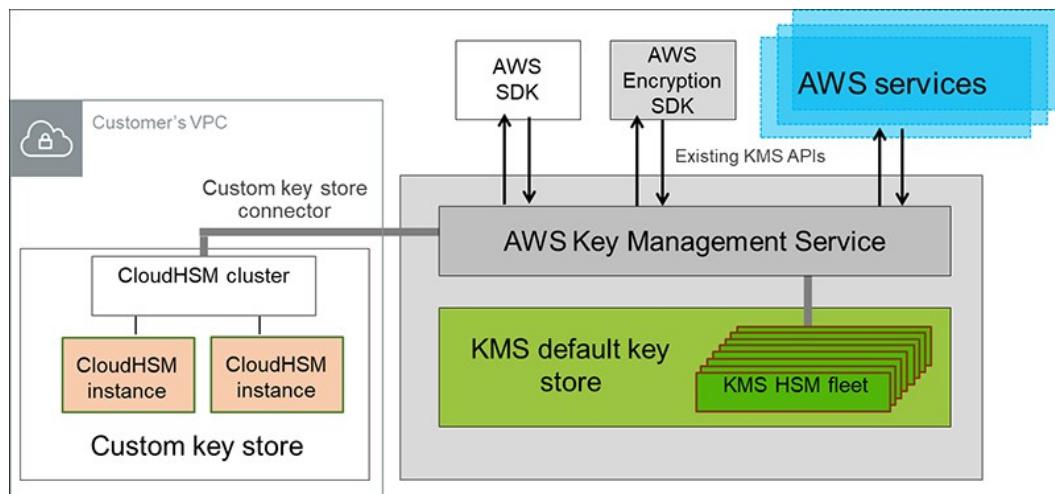
Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa precisa que todos os dados armazenados na nuvem sejam criptografados em repouso. Para integrar isso facilmente com outros serviços da AWS, é necessário ter controle total sobre a criptografia das chaves criadas e também a capacidade de remover imediatamente o material da chave do AWS KMS. A solução também deve ser capaz de auditar o uso da chave independentemente do AWS CloudTrail.

Qual das seguintes opções atenderá a esse requisito?

Use o AWS Key Management Service para criar uma chave KMS em um armazenamento de chaves personalizado e armazenar o material de chave não extraível no AWS CloudHSM.

O recurso de armazenamento de chaves personalizado **do AWS Key Management Service (KMS)** combina os controles fornecidos pelo **AWS CloudHSM** com a integração e a facilidade de uso do AWS KMS. Você pode configurar seu próprio cluster do CloudHSM e autorizar o AWS KMS a usá-lo como um armazenamento de chaves dedicado para suas chaves, em vez do armazenamento de chaves padrão do AWS KMS. Ao criar chaves no AWS KMS, você pode optar por gerar o material de chaves no seu cluster do CloudHSM. As chaves do KMS geradas no seu armazenamento de chaves personalizado nunca saem dos HSMs no cluster do CloudHSM em texto simples, e todas as operações do AWS KMS que usam essas chaves do KMS são executadas apenas nos seus HSMs.



O AWS KMS pode ajudar você a integrar-se a outros serviços da AWS para criptografar os dados armazenados nesses serviços e controlar o acesso às chaves que os descriptografam. Para remover imediatamente o material da chave do AWS KMS, você pode usar um repositório de chaves personalizado. Observe que cada repositório de chaves personalizado está associado a um cluster do AWS CloudHSM na sua conta da AWS. Portanto, quando você cria uma chave do AWS KMS em um repositório de chaves personalizado, o AWS KMS gera e armazena o material da chave não extraível para a chave do KMS em um cluster do AWS CloudHSM que você possui e gerencia. Isso também é adequado se você quiser poder auditar o uso de todas as suas chaves independentemente do AWS KMS ou do AWS CloudTrail.

Como você controla seu cluster do AWS CloudHSM, tem a opção de gerenciar o ciclo de vida das suas chaves KMS independentemente do AWS KMS. Aqui estão os critérios pelos quais você pode achar um repositório de chaves personalizado útil:

- Você tem chaves de criptografia que devem ser protegidas dentro de um módulo de segurança de hardware (HSM) dedicado sob seu controle direto, aderindo a requisitos rigorosos de locação única.
 - Você precisa ter a capacidade de revogar e remover de forma rápida e independente o material da chave do AWS KMS, exercendo controle total sobre o ciclo de vida da chave.
 - Suas obrigações de conformidade exigem auditoria e monitoramento independentes de todas as principais atividades de uso, além do registro fornecido pelo AWS KMS e pelo AWS CloudTrail.
- Portanto, a resposta correta neste cenário é: **Use o AWS Key Management Service para criar uma chave KMS em um armazenamento de chaves personalizado e armazenar o material de chave não extraível no AWS CloudHSM**.

A opção que diz: **Usar o AWS Key Management Service para criar uma chave KMS em um repositório de chaves personalizado e armazenar o material de chave não extraível no Amazon S3** está incorreta. O Amazon S3 é principalmente para fins de armazenamento geral e não oferece o nível de segurança e controle necessários para o gerenciamento de chaves criptográficas. Em vez disso, você precisa usar o AWS CloudHSM.

As opções que dizem: **Usar o AWS Key Management Service para criar chaves de propriedade da AWS e armazenar o material de chave não extraível no AWS CloudHSM** e **Usar o AWS Key Management Service para criar chaves gerenciadas pela AWS e armazenar o material de chave não extraível no AWS CloudHSM** estão incorretas porque o cenário exige principalmente que você tenha controle total sobre a criptografia da chave criada. Chaves de propriedade da AWS e chaves gerenciadas pela AWS são gerenciadas pela AWS. Além disso, essas opções não permitem que você audite o uso de chaves independentemente do AWS CloudTrail.

Referências:

<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-cloudhsm.html>

<https://aws.amazon.com/blogs/security/are-kms-custom-key-stores-right-for-you/>

Confira esta folha de dicas do AWS KMS:

<https://tutorialsdojo.com/aws-key-management-service-aws-kms/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Garanta **criptografia em repouso**
- Permita **integração com outros serviços AWS**
- Ofereça **controle total sobre as chaves**, incluindo a **remoção imediata** do material criptográfico
- Suporte **auditoria independente** do CloudTrail

O uso de uma **Custom Key Store com AWS CloudHSM** oferece:

- **Chaves gerenciadas pelo cliente** com controle total sobre o ciclo de vida do material criptográfico
- Capacidade de **remover imediatamente** o material da chave (desligando ou excluindo o HSM)
- **Auditoria independente**, pois o cliente pode configurar logs diretamente no CloudHSM
- Integração com serviços AWS como S3, RDS, EBS, etc., usando KMS

Resumo Final:

Para requisitos rigorosos de segurança e conformidade, onde é necessário **controle completo sobre as chaves de criptografia**, a melhor solução é utilizar uma **Custom Key Store com o AWS KMS e AWS CloudHSM**. Essa abordagem permite **gerenciar o material criptográfico, interromper imediatamente o uso da chave** se

necessário e **auditar operações fora do CloudTrail**, atendendo plenamente às exigências de segurança e integração da empresa.

4. PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa está migrando seus aplicativos para a AWS. Um de seus sistemas requer um banco de dados com capacidade de escala global e que lide com mudanças frequentes de esquema. O aplicativo não deve apresentar tempo de inatividade ou problemas de desempenho sempre que houver uma mudança de esquema no banco de dados. Ele também deve fornecer uma resposta de baixa latência para consultas de alto tráfego.

Qual é a solução de banco de dados mais adequada para atender a esse requisito?

Amazon DynamoDB

Antes de prosseguirmos respondendo a esta pergunta, precisamos primeiro esclarecer a definição de "**esquema**". Basicamente, a definição em inglês de esquema é: uma representação de um plano ou teoria na forma de um esboço ou modelo .

Pense em um esquema como a "estrutura" ou um "modelo" dos seus dados no seu banco de dados. Como o cenário exige que o esquema, ou a estrutura dos seus dados, mude com frequência, você precisa escolher um banco de dados que ofereça uma maneira flexível e não rígida de adicionar ou remover novos tipos de dados. Este é um exemplo clássico de escolha entre um banco de dados relacional e um banco de dados não relacional (NoSQL).

Characteristic	Relational Database Management System (RDBMS)	Amazon DynamoDB
Optimal Workloads	Ad hoc queries; data warehousing; OLAP (online analytical processing).	Web-scale applications, including social networks, gaming, media sharing, and IoT (Internet of Things).
Data Model	The relational model requires a well-defined schema, where data is normalized into tables, rows and columns. In addition, all of the relationships are defined among tables, columns, indexes, and other database elements.	DynamoDB is schemaless. Every table must have a primary key to uniquely identify each data item, but there are no similar constraints on other non-key attributes. DynamoDB can manage structured or semi-structured data, including JSON documents.
Data Access	SQL (Structured Query Language) is the standard for storing and retrieving data. Relational databases offer a rich set of tools for simplifying the development of database-driven applications, but all of these tools use SQL.	You can use the AWS Management Console or the AWS CLI to work with DynamoDB and perform ad hoc tasks. Applications can leverage the AWS software development kits (SDKs) to work with DynamoDB using object-based, document-centric, or low-level interfaces.
Performance	Relational databases are optimized for storage, so performance generally depends on the disk subsystem. Developers and database administrators must optimize queries, indexes, and table structures in order to achieve peak performance.	DynamoDB is optimized for compute, so performance is mainly a function of the underlying hardware and network latency. As a managed service, DynamoDB insulates you and your applications from these implementation details, so that you can focus on designing and building robust, high-performance applications.
Scaling	It is easiest to scale up with faster hardware. It is also possible for database tables to span across multiple hosts in a distributed system, but this requires additional investment. Relational databases have maximum sizes for the number and size of files, which imposes upper limits on scalability.	DynamoDB is designed to scale out using distributed clusters of hardware. This design allows increased throughput without increased latency. Customers specify their throughput requirements, and DynamoDB allocates sufficient resources to meet those requirements. There are no upper limits on the number of items per table, nor the total size of that table.

Um banco de dados relacional é conhecido por ter um esquema rígido, com muitas restrições e limites quanto a quais (e que tipo de) dados podem ser inseridos ou não. É usado principalmente em cenários em que é necessário suportar consultas complexas que buscam dados em diversas tabelas. É ideal para cenários em que há relacionamentos complexos entre tabelas, mas não é um banco de dados adequado para casos de uso em que é necessário um esquema flexível.

Para NoSQL, ele não é tão rígido quanto um banco de dados relacional, pois você pode adicionar ou remover facilmente linhas ou elementos na sua entrada de tabela/coleção. Ele também possui um esquema mais flexível, pois pode armazenar dados hierárquicos complexos em um único item, o que, ao contrário de um banco de dados relacional, não envolve a alteração de várias tabelas relacionadas. Portanto, a melhor resposta a ser usada aqui é um banco de dados NoSQL, como o DynamoDB. Quando sua empresa exige uma resposta de baixa latência para consultas de alto tráfego, aproveitar as vantagens de um sistema NoSQL geralmente faz sentido técnico e econômico.

O Amazon DynamoDB ajuda a solucionar os problemas que limitam a escalabilidade do sistema relacional, evitando-os. No DynamoDB, você projeta seu esquema especificamente para tornar as consultas mais comuns e importantes o mais rápidas e econômicas possível. Suas estruturas de dados são adaptadas aos requisitos específicos dos seus casos de uso de negócios.

Lembre-se de que um sistema de banco de dados relacional **não é** bem escalável pelos seguintes motivos:

- Ele normaliza os dados e os armazena em várias tabelas que exigem várias consultas para gravar no disco.
- Geralmente incorre nos custos de desempenho de um sistema de transação compatível com ACID.
- Ele usa junções caras para remontar as visualizações necessárias dos resultados da consulta.

O **DynamoDB** é bem escalável pelos seguintes motivos:

- A **flexibilidade do esquema** permite que o DynamoDB armazene dados hierárquicos complexos em um único item. O DynamoDB não é um banco de dados totalmente sem esquema, pois a própria definição de esquema é apenas o modelo ou a estrutura dos seus dados.
- O design de chave composta permite armazenar itens relacionados próximos uns dos outros na mesma tabela.

Uma instância do Amazon RDS na configuração de implantações Multi-AZ e um banco de dados Amazon Aurora com réplicas de leitura estão s porque ambos são um tipo de banco de dados relacional.

Redshift está porque é usado principalmente para sistemas OLAP.

Referências:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-general-nosql-design.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-relational-modeling.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.html>

Confira também o **Guia de Estudo Oficial do AWS Certified Solutions Architect: Exame Associado 1^a Edição** e vá para a página 161 que fala sobre bancos de dados NoSQL.

Confira esta folha de dicas do Amazon DynamoDB:

<https://tutorialsdojo.com/amazon-dynamodb>

Guia de estudo para o exame AWS Certified Solutions Architect Associate da Tutoriais Dojo:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Escale globalmente
- Suporte mudanças frequentes de esquema
- Não gere downtime ou degradação de performance com mudanças
- Atenda grandes volumes de tráfego com **baixa latência**

O Amazon DynamoDB é:

- Um banco de dados NoSQL **gerenciado**, com **arquitetura serverless**
 - **Altamente escalável globalmente** com o recurso Global Tables
 - **Esquema flexível**, permitindo alterações sem interrupção ou reestruturação
 - Projetado para **baixa latência de milissegundos**, mesmo sob carga pesada
 - Ideal para aplicações modernas que exigem **alta disponibilidade e desempenho**
-

Resumo Final:

Para sistemas que exigem **alta escalabilidade, baixa latência, alta disponibilidade e mudanças frequentes de esquema sem downtime**, o **Amazon DynamoDB** é a escolha ideal. Seu modelo NoSQL flexível e gerenciado permite escalar globalmente sem comprometer a performance, atendendo perfeitamente às demandas modernas de aplicações em nuvem.

5. PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma plataforma de negociação de criptomoedas utiliza uma API construída em AWS Lambda e API Gateway. Devido às notícias e rumores recentes sobre a iminente alta de preços do Bitcoin, Ethereum e outras criptomoedas, espera-se que a plataforma de negociação tenha um aumento significativo de visitantes e novos usuários nos próximos dias.

Nesse cenário, como você pode proteger os sistemas de backend da plataforma contra picos de tráfego?

Habilite limites de limitação e armazenamento em cache de resultados no API Gateway.

O **Amazon API Gateway** oferece controle de fluxo em vários níveis, incluindo global e por chamada de serviço. Limites de controle de fluxo podem ser definidos para taxas e picos padrão. Por exemplo, os proprietários de APIs podem definir um limite de taxa de 1.000 solicitações por segundo para um método específico em suas APIs REST e também configurar o Amazon API Gateway para lidar com um pico de 2.000 solicitações por segundo por alguns segundos. O Amazon API Gateway rastreia o número de solicitações por segundo. Qualquer solicitação acima do limite receberá uma resposta HTTP 429. Os SDKs de cliente gerados pelo Amazon API Gateway repetem as chamadas automaticamente quando recebem essa resposta. Portanto, **habilitar os limites de controle de fluxo e o cache de resultados no API Gateway** é a resposta correta.

Você pode adicionar cache às chamadas de API provisionando um cache do Amazon API Gateway e especificando seu tamanho em gigabytes. O cache é provisionado para um estágio específico das suas APIs. Isso melhora o desempenho e reduz o tráfego enviado ao seu back-end. As configurações de cache permitem controlar a forma como a chave de cache é criada e o tempo de vida (TTL) dos dados armazenados para cada método. O Amazon API Gateway também expõe APIs de gerenciamento que ajudam a invalidar o cache para cada estágio.

prod Stage Editor

Invoke URL: <https://execute-api.us-east-2.amazonaws.com/prod>

Settings Logs Stage Variables SDK Generation Export Deployment History Documentation History Canary

Configure the metering and caching settings for the **prod** stage.

Cache Settings

Enable API cache

Default Method Throttling

Choose the default throttling level for the methods in this stage. Each method in this stage will respect these rate and burst settings. Your current account level throttling rate is **10000** requests per second with a burst of **5000** requests. [Read more about API Gateway throttling](#)

Enable throttling i

Rate requests per second

Burst requests

Client Certificate

A opção que diz: **Mudar de uso do AWS Lambda e API Gateway para uma arquitetura mais escalável e altamente disponível usando instâncias EC2, ELB e Auto Scaling** está incorreta, pois não há necessidade de transferir seus aplicativos para outros serviços.

Usar o CloudFront antes do API Gateway para atuar como cache é , pois o CloudFront apenas acelera a entrega de conteúdo, o que proporciona uma melhor experiência de latência para os usuários. Isso não ajuda muito o backend.

Mover a função Lambda para uma VPC está porque esta resposta é irrelevante para o que está sendo perguntado. Uma VPC é sua própria nuvem privada virtual, onde você pode iniciar serviços da AWS.

Referência :

<https://aws.amazon.com/api-gateway/faqs/>

Confira esta folha de dicas do Amazon API Gateway:

<https://tutorialsdojo.com/amazon-api-gateway/>

Justificativa:

A pergunta exige uma solução que:

- Proteja o backend (Lambda e outros serviços) contra **sobrecarga em momentos de pico**
- **Reduza a latência e melhora a experiência do usuário**
- Mantenha **resiliência e escalabilidade** sob demanda variável

O uso de throttling e caching no API Gateway:

- **Throttling** limita o número de requisições por segundo, **evitando sobrecarga** nas funções Lambda e nos sistemas downstream

- **Caching** armazena temporariamente as respostas de APIs, **reduzindo chamadas repetitivas ao backend**
- Ambos os recursos são **fáceis de configurar diretamente no API Gateway**
- **Reduzem custos**, já que evitam execuções desnecessárias do Lambda
- Melhoram a **performance e estabilidade** em cenários de tráfego explosivo

Resumo Final:

Para lidar com aumentos repentinos de tráfego, **limitar requisições por segundo (throttling)** e **habilitar cache de resposta no API Gateway** são estratégias altamente eficazes. Essas práticas ajudam a proteger o backend contra picos de carga, melhoram o desempenho percebido pelo usuário e mantêm a aplicação funcionando de forma estável e econômica.

6. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Um Arquiteto de Soluções está projetando uma solução de banco de dados relacional de alta disponibilidade para mitigar o risco de falha multirregional. O banco de dados deve atender a um Objetivo de Ponto de Recuperação (RPO) de 1 segundo e um Objetivo de Tempo de Recuperação (RTO) de menos de 1 minuto. O arquiteto precisa de um plano de recuperação de desastres que permita a replicação automática entre regiões com perda mínima de dados e recuperação rápida em caso de falha. Qual recurso da AWS atende melhor a esse requisito?

Banco de dados global do Amazon Aurora

O **Amazon Aurora Global Database** foi projetado para aplicações distribuídas globalmente, permitindo que um único banco de dados Amazon Aurora abranja várias regiões da AWS. Ele replica seus dados sem afetar o desempenho do banco de dados, permite leituras locais rápidas com baixa latência em cada região e fornece recuperação de desastres em caso de interrupções em toda a região.

The screenshot shows the Amazon RDS console with the 'Databases' page selected. On the left, there's a sidebar with various navigation options like Dashboard, Databases, Query Editor, etc. The main area displays a table of databases. A red box highlights the second database cluster, 'global-database-2'. This cluster is listed under 'Global' and 'Aurora PostgreSQL'. It has 2 regions: 'us-east-1' and 'us-east-2'. Under 'us-east-1', it shows 1 instance (Primary) and 1 instance (Secondary). Under 'us-east-2', it shows 1 instance (Reader). The table includes columns for DB Identifier, Role, Engine, Region & AZ, Size, Status, CPU, and Current activity.

DB Identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity
global-database-1	Global	Aurora MySQL	1 region	1 cluster	Available	-	-
global-database-1-cluster-1	Primary	Aurora MySQL	us-east-1	1 instance	Available	-	-
global-database-1-instance-1	Writer	Aurora MySQL	us-east-1a	db.r5.large	Available	-	-
global-database-2	Global	Aurora PostgreSQL	2 regions	2 clusters	Available	-	-
global-database-2-cluster-1	Primary	Aurora PostgreSQL	us-east-1	1 instance	Available	-	-
global-database-2-instance-1	Writer	Aurora PostgreSQL	us-east-1d	db.r5.2xlarge	Available	-	-
global-database-2-cluster-1	Secondary	Aurora PostgreSQL	us-east-2	1 instance	Available	-	-
global-database-2-instance-1	Reader	Aurora PostgreSQL	us-east-2c	db.r5.2xlarge	Available	0.00%	-

O Aurora Global Database suporta replicação baseada em armazenamento com latência inferior a 1 segundo. Em caso de interrupção não planejada, uma das regiões secundárias atribuídas pode ser promovida para capacidades de leitura e gravação em menos de 1 minuto. Esse recurso é chamado de

Recuperação de Desastres entre Regiões. Um RPO de 1 segundo e um RTO de menos de 1 minuto fornecem uma base sólida para um plano global de continuidade de negócios.

Portanto, a resposta correta é: **Amazon Aurora Global Database**.

A opção que diz: **Tabela global do Amazon DynamoDB** está incorreta porque, embora suporte tabelas multirregionais totalmente replicadas com baixa latência, ela é mais adequada para cargas de trabalho NoSQL, não para bancos de dados relacionais.

A opção que diz: **Amazon RDS para PostgreSQL com réplicas de leitura entre regiões** está incorreta. Embora essa opção possa ajudar na recuperação de desastres, ela simplesmente não atende aos requisitos de RPO e RTO especificados no cenário. O atraso na replicação em réplicas de leitura entre regiões pode levar vários minutos para ser concluído, o que pode impedir a empresa de atingir o RPO de 1 segundo.

A opção que diz: **Amazon Timestream for Analytics** está incorreta porque se trata principalmente de um serviço de banco de dados de séries temporais sem servidor, comumente usado para IoT e aplicações operacionais. A solução mais adequada para este cenário é usar o Amazon Aurora Global Database, pois ele pode fornecer o RPO e o RTO necessários.

Referências:

<https://aws.amazon.com/rds/aurora/global-database/>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Confira esta folha de dicas do Amazon Aurora:

<https://tutorialsdojo.com/amazon-aurora/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE OFEREÇA:

- Alta disponibilidade multirregional
- RPO de 1 segundo
- RTO inferior a 1 minuto
- Replicação automática entre regiões
- Recuperação de desastres com mínima perda de dados

O Amazon Aurora Global Database é:

- Projetado especificamente para replicação entre regiões com latência inferior a 1 segundo
- Capaz de atingir RPO de ~1 segundo e RTO inferior a 1 minuto
- Ideal para recuperação de desastres com failover rápido entre regiões
- Gerenciado pela AWS, com baixa sobrecarga operacional
- Baseado em infraestrutura distribuída e altamente resiliente do Aurora

Resumo Final:

Para workloads críticos que exigem recuperação quase imediata e mínima perda de dados em cenários de falha regional, o **Aurora Global Database** é a melhor escolha. Ele oferece replicação automática, rápida e segura entre regiões da AWS, atingindo os exigentes objetivos de RPO e RTO. Além disso, elimina a

complexidade de gerenciar replicação manual ou scripts de failover, sendo uma solução altamente confiável e eficaz para **disaster recovery** multirregional.

7. PERGUNTA

Categoria: CSAA - Design de Arquiteturas de Alto Desempenho

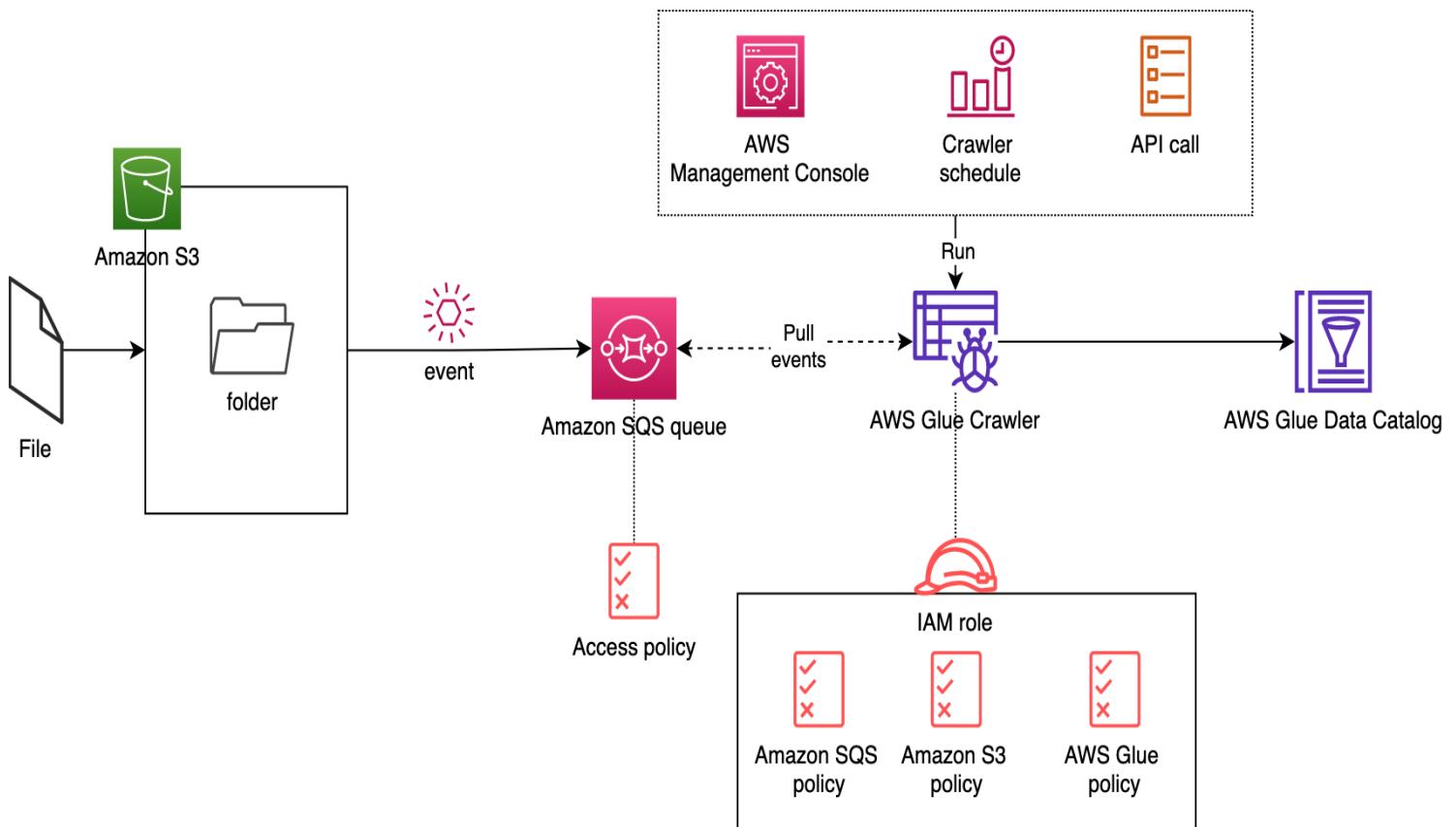
Uma empresa de varejo recebe **.csv** arquivos de dados brutos em seu bucket do Amazon S3 de diversas fontes a cada hora, com um tamanho médio de arquivo de 2 GB.

Um processo automatizado deve ser implementado para converter esses **.csv** arquivos para o formato mais eficiente do Apache Parquet e armazenar os arquivos convertidos em outro bucket do S3. Além disso, o processo de conversão deve ser iniciado automaticamente sempre que um novo arquivo for carregado no bucket do S3.

Qual das seguintes opções deve ser implementada para atender a esses requisitos com a **MENOR** sobrecarga operacional?

Utilize uma tarefa de extração, transformação e carregamento (ETL) do AWS Glue para processar e converter os **.csv arquivos para o formato Apache Parquet e, em seguida, armazenar os arquivos de saída no bucket S3 de destino. Configure uma Notificação de Eventos do S3 para rastrear cada **S3 PUT** evento e invocar a tarefa ETL no Glue por meio do Amazon SQS.**

O AWS Glue é um serviço de ETL poderoso que move dados facilmente entre diferentes repositórios de dados. Usando o AWS Glue, você pode criar e gerenciar facilmente tarefas de ETL para transferir dados de diversas fontes, como Amazon S3, Amazon RDS e Amazon Redshift. Além disso, o AWS Glue permite transformar seus dados conforme necessário para atender às suas necessidades específicas. Uma das principais vantagens do AWS Glue é a descoberta e o mapeamento automáticos de esquemas, que permitem mapear facilmente dados de diferentes fontes com diferentes esquemas.



Ao trabalhar com processamento de big data, muitas vezes é necessário converter dados de um formato para outro para otimizar a eficiência do processamento. O Apache Parquet é um formato de armazenamento em colunas projetado para fornecer maior eficiência e desempenho para processamento de big data. Ao armazenar e processar grandes quantidades de dados com altas taxas de compactação e tempos de consulta mais rápidos, o Parquet pode oferecer benefícios significativos para a empresa. Felizmente, o Parquet

é compatível com muitas estruturas de processamento de dados, como Spark, Hive e Hadoop, tornando-o um formato versátil para processamento de big data. Usando o AWS Glue e outros serviços da AWS, você pode facilmente converter seus arquivos .csv para o formato mais eficiente do Apache Parquet e armazenar os arquivos de saída em um bucket S3, facilitando o acesso e o processamento de grandes quantidades de dados.

Portanto, a resposta correta é: **utilize uma tarefa de extração, transformação e carregamento (ETL) do AWS Glue para processar e converter os .csv arquivos para o formato Apache Parquet e, em seguida, armazenar os arquivos de saída no bucket S3 de destino. Configure uma Notificação de Eventos do S3 para rastrear cada S3 PUT evento e invocar a tarefa ETL no Glue por meio do Amazon SQS.**

A opção que diz: **Usar uma função do AWS Lambda acionada por um S3 PUT evento para converter os .csv arquivos para o formato Parquet. Usar o serviço AWS Transfer Family com SFTP para mover os arquivos de saída para o bucket S3 de destino** está incorreta. A conversão dos arquivos CSV para o formato Parquet usando uma combinação de uma função Lambda e notificação de eventos S3 funcionaria; no entanto, esta não é a solução mais eficiente ao lidar principalmente com grandes quantidades de dados. A função Lambda tem um limite máximo de tempo de execução, o que significa que a conversão de arquivos grandes pode resultar em problemas de tempo limite. Usar o serviço AWS Transfer Family com SFTP para mover os arquivos de saída para o bucket S3 de destino também é desnecessário. Além disso, a leitura dos registros precisa ser entregue por meio de um fluxo de dados, pois uma função Lambda tem um limite de memória. Isso implica um esforço adicional em comparação com o uso do AWS Glue.

A opção que diz: **Configurar um job do Apache Spark em execução em uma instância do Amazon EC2 e criar uma regra do Amazon EventBridge (Amazon CloudWatch Events) para monitorar S3 PUT eventos no bucket do S3. Configurar o AWS Lambda para invocar o job do Spark para cada novo .csv arquivo adicionado por meio de uma URL de função** está incorreta. Executar o Spark em instâncias do EC2 requer provisionamento, monitoramento e manutenção manuais, o que gera tempo e custos adicionais. Além disso, usar o Amazon EventBridge (Amazon CloudWatch Events) para acionar o job do Spark por meio de uma URL de função adiciona complexidade e potenciais pontos de falha. Portanto, essa opção apenas introduz complexidade desnecessária e sobrecarga operacional.

A opção que diz: **Criar uma tarefa ETL (Extraír, Transformar, Carregar) e uma tabela do Catálogo de Dados no AWS Glue. Configurar o rastreador do Glue para ser executado de acordo com uma programação para verificar novos arquivos no bucket do S3 a cada hora e convertê-los para o formato Parquet** está incorreta. Embora seja correto criar uma tarefa ETL usando o AWS Glue, simplesmente acionar a tarefa de forma programada, em vez de ser acionada automaticamente por um novo upload de arquivo, não é o ideal. Não é tão eficiente quanto usar um gatilho de evento do S3 para iniciar o processo de conversão imediatamente após o upload do arquivo.

Referências:

<https://aws.amazon.com/blogs/big-data/executar-crawlers-de-glue-da-aws-usando-notificações-de-eventos-do-amazon-s3/>

<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-parquet-home.html>

<https://docs.aws.amazon.com/athena/latest/ug/glue-athena.html>

Confira esta folha de dicas do AWS Glue:

<https://tutorialsdojo.com/aws-glue/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Converta arquivos .csv automaticamente em Parquet
- Inicie o processo ao detectar novos uploads no S3
- Tenha **baixa sobrecarga operacional**
- Armazene os resultados em outro bucket do S3

A combinação S3 + SQS + AWS Glue oferece:

- **Automação total** com eventos do S3 ativando a tarefa ETL via SQS
 - O **AWS Glue** é totalmente gerenciado e especializado em tarefas de ETL com conversão entre formatos como CSV e Parquet
 - O formato **Apache Parquet** é otimizado para análise, reduzindo custo de armazenamento e aumentando performance em consultas
 - **Baixa complexidade operacional**, já que todos os componentes são gerenciados pela AWS e integrados entre si
 - **Alta escalabilidade** para processar arquivos de grande volume (2 GB+)
-

Resumo Final:

Para processar e converter automaticamente arquivos CSV em Parquet com **menor esforço operacional**, a melhor solução é usar o **AWS Glue ETL**, disparado por **eventos do S3 via SQS**. Essa arquitetura elimina a necessidade de servidores, é escalável e aproveita ao máximo os serviços gerenciados da AWS, proporcionando eficiência, automação e baixo custo de manutenção.

8. PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa de tecnologia possui um aplicativo de CRM hospedado em um grupo de Auto Scaling de instâncias EC2 sob demanda com diferentes tipos e tamanhos de instância. O aplicativo é amplamente utilizado durante o horário comercial, das 9h às 17h. Os usuários reclamam que o desempenho do aplicativo é lento no início do dia, mas volta a funcionar normalmente após algumas horas. Qual das seguintes opções é a solução operacional **MAIS** eficiente a ser implementada para garantir que o aplicativo funcione corretamente no início do dia?

Configure uma política de dimensionamento agendado para o grupo de dimensionamento automático para iniciar novas instâncias antes do início do dia.

O escalonamento baseado em um cronograma permite que você escale seu aplicativo em resposta a mudanças previsíveis de carga. Por exemplo, toda semana, o tráfego para seu aplicativo web começa a aumentar na quarta-feira, permanece alto na quinta-feira e começa a diminuir na sexta-feira. Você pode planejar suas atividades de escalonamento com base nos padrões previsíveis de tráfego do seu aplicativo web.

AWS Services Search [Option+S] N. Virginia Tutorials Dojo

New EC2 Experience Tell us what you think X

EC2 > Auto Scaling groups > Agila Scheduled actions

Agila Create scheduled action

Scheduled scaling helps you

Name: Scheduled Auto Scaling – Tutorials Dojo

Provide at least one value for Desired, Min, or Max Capacity

Desired capacity: 10, Min: 2, Max: 30

Recurrence: Every day (Cron) 0 0 * * *

Time zone: Singapore

Specific start time: 2023/08/06 00:00 Singapore

End by: 2022/12/05 00:00 Singapore

Cancel Learn more about scheduled scaling

Scheduled actions Cancel Create

Actions Create scheduled action Filter scheduled actions



Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy Terms Cookie preferences

Para configurar seu grupo de Auto Scaling para escalar com base em uma programação, crie uma ação programada. A ação programada instrui o Amazon EC2 Auto Scaling a executar uma ação de escala em horários específicos. Para criar uma ação de escala programada, especifique o horário de início em que a ação de escala entrará em vigor e os novos tamanhos mínimo, máximo e desejado para a ação de escala. No horário especificado, o Amazon EC2 Auto Scaling atualiza o grupo com os valores de tamanho mínimo, máximo e desejado especificados pela ação de escala. Você pode criar ações programadas para escalar apenas uma vez ou para escalar em uma programação recorrente.

Portanto, **configurar uma política de escalonamento agendada para que o grupo de escalonamento automático inicie novas instâncias antes do início do dia** é a solução correta. Você precisa configurar uma política de escalonamento agendada. Isso garantirá que as instâncias já estejam escalonadas e prontas antes do início do dia, pois é quando o aplicativo é mais utilizado.

As opções a seguir estão incorretas. Embora sejam soluções válidas, ainda é melhor configurar uma política de escalonamento agendada, pois você já sabe os horários de pico exatos do seu aplicativo. Quando a CPU ou a memória atingem o pico, o aplicativo já apresenta problemas de desempenho, portanto, você precisa garantir que o escalonamento seja feito previamente usando uma política de escalonamento agendada:

- Configurar uma política de dimensionamento dinâmico para o grupo de dimensionamento automático para iniciar novas instâncias com base na utilização da CPU

- Configurar uma política de dimensionamento dinâmico para o grupo de dimensionamento automático para iniciar novas instâncias com base na utilização de memória

A opção que diz: **Configurar uma política de dimensionamento preditivo para o grupo de dimensionamento automático para ajustar automaticamente o número de instâncias do Amazon EC2** está incorreta. Embora esse tipo de política de dimensionamento possa ser usado neste cenário, não é a opção mais eficiente operacionalmente. Observe que o cenário mencionou que o grupo de dimensionamento automático consiste em instâncias do Amazon EC2 com diferentes tipos e tamanhos de instância. O dimensionamento preditivo pressupõe que seu grupo de dimensionamento automático seja homogêneo, o que significa que todas as instâncias do EC2 têm a mesma capacidade. A capacidade prevista pode ser imprecisa se você estiver usando uma variedade de tamanhos e tipos de instâncias do EC2 em seu grupo de dimensionamento automático.

Referências:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html#predictive-scaling-limitations>

Confira esta folha de dicas de dimensionamento automático da AWS:

<https://tutorialsdojo.com/aws-auto-scaling/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Resolva problemas de **baixa performance no início do expediente**
- Seja **operacionalmente eficiente**
- Considere um uso **previsível e repetitivo** (uso intenso das 9h às 17h)

A política de dimensionamento agendado:

- Permite **aumentar a capacidade antes de um pico esperado**
- Garante que as instâncias EC2 estejam **prontas e aquecidas** quando os usuários começarem a usar o sistema
- Evita atrasos causados pelo **aquecimento lento** do Auto Scaling dinâmico baseado em métricas
- É **simples de configurar**, sem necessidade de monitoramento contínuo
- Usa recursos nativos do Auto Scaling e **não adiciona custos extras**

Resumo Final:

Para cargas de trabalho previsíveis com picos conhecidos, como um aplicativo de CRM usado em horário comercial, o uso de **dimensionamento agendado** é a solução mais eficiente. Ele permite preparar o

ambiente com antecedência, garantindo **melhor desempenho no início do dia** e proporcionando **experiência consistente aos usuários**, com **mínima complexidade operacional**.

9. PREGUNTA

Categoría: CSAA - Design de Arquiteturas de Alto Desempenho

Uma startup está usando o Amazon RDS para armazenar dados de um aplicativo web. Na maioria das vezes, o aplicativo tem baixa atividade do usuário, mas recebe picos de tráfego em segundos sempre que há um anúncio de novo produto. O Arquiteto de Soluções precisa criar uma solução que permita que usuários em todo o mundo acessem os dados usando uma API.

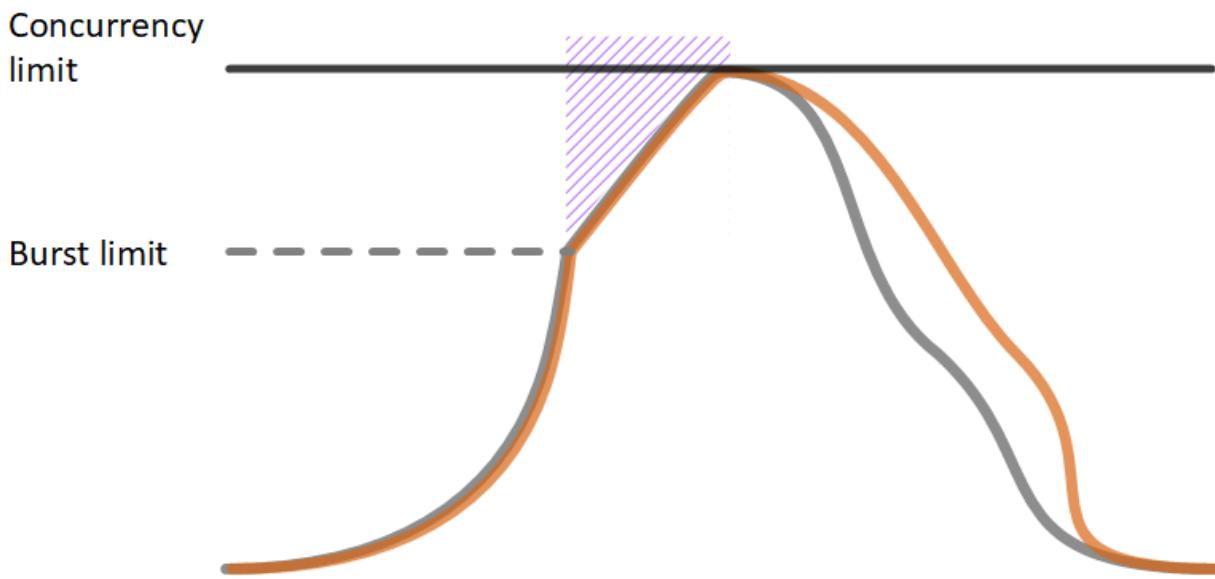
O que o Arquiteto de Soluções deve fazer para atender ao requisito acima?

Crie uma API usando o Amazon API Gateway e use o AWS Lambda para lidar com os picos de tráfego em segundos.

O **AWS Lambda** permite que você execute código sem provisionar ou gerenciar servidores. Você paga apenas pelo tempo de computação consumido. Com o Lambda, você pode executar código para praticamente qualquer tipo de aplicação ou serviço de back-end - tudo sem necessidade de administração. Basta enviar seu código e o Lambda cuida de tudo o que é necessário para executar e escalar seu código com alta disponibilidade. Você pode configurar seu código para ser acionado automaticamente a partir de outros serviços da AWS ou chamá-lo diretamente de qualquer aplicativo web ou móvel.

Na primeira vez que você invoca sua função, o AWS Lambda cria uma instância dela e executa seu método manipulador para processar o evento. Quando a função retorna uma resposta, ela permanece ativa e aguarda para processar eventos adicionais. Se você invocar a função novamente enquanto o primeiro evento estiver sendo processado, o Lambda inicializa outra instância e processa os dois eventos simultaneamente. À medida que mais eventos chegam, o Lambda os encaminha para instâncias disponíveis e cria novas instâncias conforme necessário. Quando o número de solicitações diminui, o Lambda interrompe instâncias não utilizadas para liberar capacidade de escala para outras funções.

Function Scaling with Concurrency Limit



A simultaneidade das suas funções é o número de instâncias que atendem a solicitações em um determinado momento. Para um pico inicial de tráfego, a simultaneidade cumulativa das suas funções em uma região pode atingir um nível inicial entre 500 e 3.000, que varia de acordo com a região.

Com base no cenário apresentado, você precisa criar uma solução que atenda aos dois requisitos. O primeiro requisito é criar uma solução que permita aos usuários acessar os dados usando uma API. Para implementar essa solução, você pode usar o Amazon API Gateway. O segundo requisito é lidar com o pico de tráfego em segundos. Você deve usar o AWS Lambda neste cenário, pois as funções do Lambda podem absorver picos razoáveis de tráfego por aproximadamente 15 a 30 minutos.

O Lambda pode escalar mais rápido do que o recurso de Auto Scaling padrão do Amazon EC2, Amazon Elastic Beanstalk ou Amazon ECS. Isso ocorre porque o AWS Lambda é mais leve do que outros serviços de computação. Internamente, o Lambda pode executar seu código em milhares de instâncias do EC2 gerenciadas pela AWS (que podem já estar em execução) em segundos para acomodar o tráfego. Isso é mais rápido do que o processo de Auto Scaling para iniciar novas instâncias do EC2, que pode levar alguns minutos. Uma alternativa é provisionar excessivamente sua capacidade computacional, mas isso incorrerá em custos significativos. A melhor opção para implementar, considerando os requisitos, é uma combinação do AWS Lambda e do Amazon API Gateway.

Portanto, a resposta correta é: **crie uma API usando o Amazon API Gateway e use o AWS Lambda para lidar com os picos de tráfego.**

A opção que diz: **Criar uma API usando o Amazon API Gateway e usar o cluster do Amazon ECS com o Service Auto Scaling para lidar com picos de tráfego em segundos** está incorreta. O AWS Lambda é uma opção melhor que o Amazon ECS, pois pode lidar com picos repentinos de tráfego em segundos, e não em minutos.

A opção que diz: **Criar uma API usando o Amazon API Gateway e usar o Amazon Elastic Beanstalk com Auto Scaling para lidar com os picos de tráfego em segundos** está incorreta porque, assim como a opção anterior, o uso do Auto Scaling tem um atraso de alguns minutos, pois inicia novas instâncias do EC2 que serão usadas pelo Amazon Elastic Beanstalk.

A opção que diz: **Criar uma API usando o Amazon API Gateway e usar um grupo de Auto Scaling de instâncias do Amazon EC2 para lidar com picos de tráfego em segundos** está incorreta porque o tempo de processamento do Auto Scaling do Amazon EC2 para provisionar novos recursos leva minutos. Observe que, nesse cenário, espera-se que ocorra um pico de tráfego em segundos.

Referências:

<https://aws.amazon.com/blogs/startups/de-0-a-100-k-em-segundos-escala-instantânea-com-aws-lambda/>
[https://docs.aws.amazon.com/lambda/latest/dg\(invocation-scaling.html](https://docs.aws.amazon.com/lambda/latest/dg(invocation-scaling.html)

Confira esta folha de dicas do AWS Lambda:

<https://tutorialsdojo.com/aws-lambda/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Atenda a uma aplicação com tráfego altamente variável (baixo uso usual e picos repentinos)
- Ofereça acesso global via API
- Seja escalável e gerencie os picos de forma automática

O Amazon API Gateway com AWS Lambda:

- Permite criar APIs escaláveis e gerenciadas sem servidor (serverless)
- O Lambda escala automaticamente para atender picos repentinos de requisições
- Reduz a necessidade de gerenciar servidores ou infraestrutura
- Fornece alta disponibilidade e baixa latência globalmente

Resumo Final:

Para um cenário com tráfego imprevisível e picos repentinos, a combinação do Amazon API Gateway com AWS Lambda oferece uma solução escalável, gerenciada e econômica. Essa arquitetura serverless permite que a startup responda rapidamente ao aumento da demanda global, sem comprometer desempenho ou custo, atendendo perfeitamente ao requisito do projeto.

10. PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

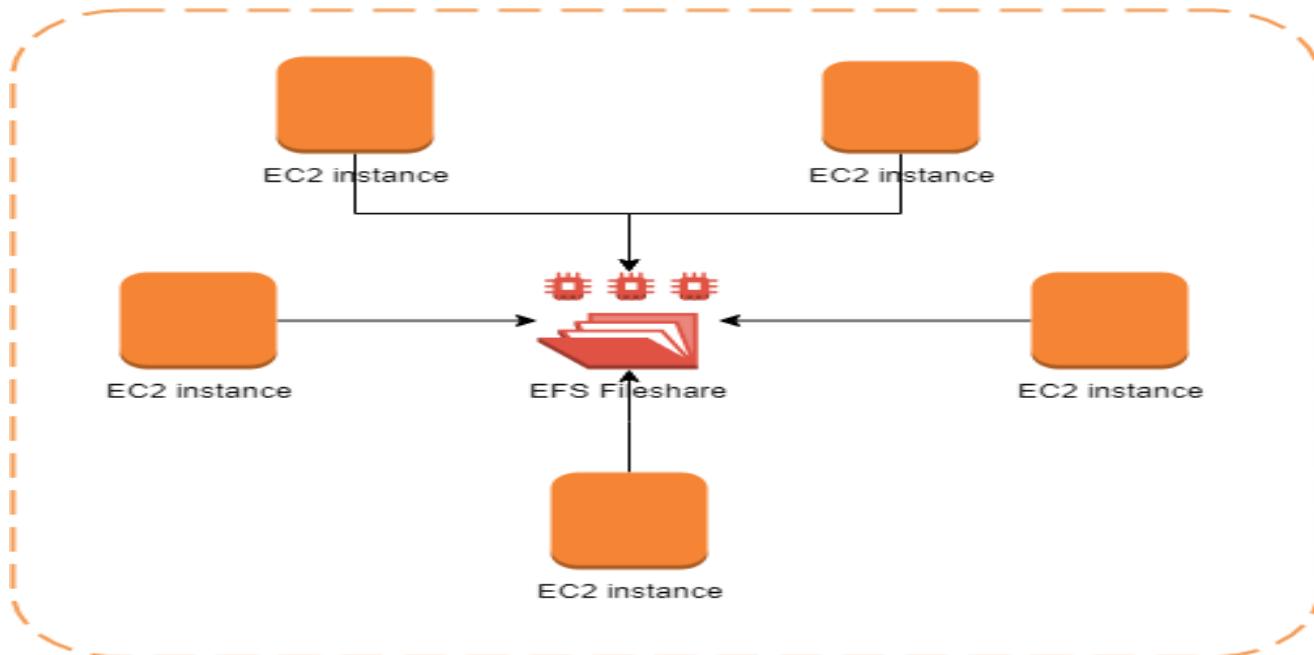
Um sistema de gerenciamento de conteúdo (CMS) está hospedado em uma frota de instâncias do Amazon EC2 sob demanda e autoescaláveis que usam o Amazon Aurora como banco de dados. Atualmente, o sistema armazena os documentos de arquivo que os usuários carregam em um dos volumes do Amazon EBS anexados. O desempenho do sistema tem sido observado como lento, e o gerente instruiu a equipe a aprimorar a arquitetura.

Nesse cenário, qual solução deve ser implementada para obter um sistema de arquivos compartilhados escalável, altamente disponível e compatível com POSIX?

Use o Amazon EFS para fornecer um sistema de arquivos compartilhado para acesso simultâneo aos dados

O **Amazon Elastic File System (Amazon EFS)** oferece armazenamento de arquivos simples, escalável e elástico para uso com serviços da Nuvem AWS e recursos locais. Quando montado em instâncias do Amazon EC2, um sistema de arquivos do Amazon EFS fornece uma interface de sistema de arquivos padrão e semântica de acesso ao sistema de arquivos, permitindo a integração perfeita do Amazon EFS com seus aplicativos e ferramentas existentes. Várias instâncias do Amazon EC2 podem acessar um sistema de arquivos do Amazon EFS simultaneamente, permitindo que o Amazon EFS forneça uma fonte de dados comum para cargas de trabalho e aplicativos executados em mais de uma instância do Amazon EC2.

Este cenário específico testa seus conhecimentos sobre EBS, EFS e S3. Neste cenário, há uma frota de instâncias do EC2 sob demanda que armazenam documentos de arquivo dos usuários em um dos volumes do EBS anexados. O desempenho do sistema é bastante lento porque a arquitetura não fornece às instâncias do EC2 acesso compartilhado paralelo aos documentos de arquivo.



Embora um volume EBS possa ser anexado a várias instâncias do EC2, isso só é possível em instâncias dentro de uma zona de disponibilidade. O que precisamos é de armazenamento de alta disponibilidade que possa abranger várias zonas de disponibilidade. Observe também que o tipo de armazenamento necessário aqui é o armazenamento de arquivos, o que significa que o S3 não é o melhor serviço a ser usado, pois é usado principalmente para armazenamento de objetos.

Portanto, a resposta correta é: **Use o Amazon EFS para fornecer um sistema de arquivos compartilhado para acesso simultâneo aos dados**.

A opção que diz: **Criar um bucket do Amazon S3 e usá-lo como armazenamento para o CMS** está incorreta porque o Amazon S3 é apenas um serviço de armazenamento de objetos, que não fornece a interface de sistema de arquivos nem o bloqueio de arquivos necessários para um CMS.

A opção que diz: **Atualize seus volumes EBS existentes para volumes SSD com IOPS provisionados** está incorreta, pois a simples atualização do EBS não atende ao requisito de um sistema de arquivos compartilhado compatível com POSIX. Os volumes EBS são dispositivos de armazenamento em bloco conectados a uma única instância, o que os torna inadequados para armazenamento compartilhado.

A opção que diz: **Aproveite o Amazon ElastiCache para armazenar em cache dados acessados com frequência e reduzir a latência** está incorreta porque esse é um armazenamento de dados na memória que melhora o desempenho dos seus aplicativos, o que não é o que você precisa, já que não é um armazenamento de arquivos.

Referências:

<https://aws.amazon.com/efs/>

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

<https://docs.aws.amazon.com/efs/latest/ug/mount-multiple-ec2-instances.html>

Confira esta folha de dicas do Amazon EFS:

<https://tutorialsdojo.com/amazon-efs/>

Confira esta folha de dicas do Amazon S3 vs EBS vs EFS:

<https://tutorialsdojo.com/amazon-s3-vs-ebs-vs-efs/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Ofereça um sistema de arquivos compartilhado para múltiplas instâncias EC2
- Seja escalável e altamente disponível
- Seja compatível com o padrão POSIX (permitindo operações de arquivo típicas)
- Melhore o desempenho e a arquitetura atual

O Amazon EFS:

- Proporciona um sistema de arquivos **nativo, gerenciado e escalável**
- Suporta acesso simultâneo e consistente a arquivos por várias instâncias EC2
- É altamente disponível e durável, com replicação automática entre zonas de disponibilidade
- Compatível com POSIX, permitindo que aplicações que dependem dessa compatibilidade funcionem corretamente
- Resolve o problema de armazenamento distribuído, eliminando o uso inadequado de volumes EBS locais que não são compartilhados

Resumo Final:

Para sistemas distribuídos e autoescaláveis que precisam acessar arquivos compartilhados, o Amazon EFS é a solução ideal. Ele oferece escalabilidade, alta disponibilidade e compatibilidade POSIX,

melhorando significativamente o desempenho e a confiabilidade da aplicação em comparação ao uso de volumes EBS anexados individualmente.

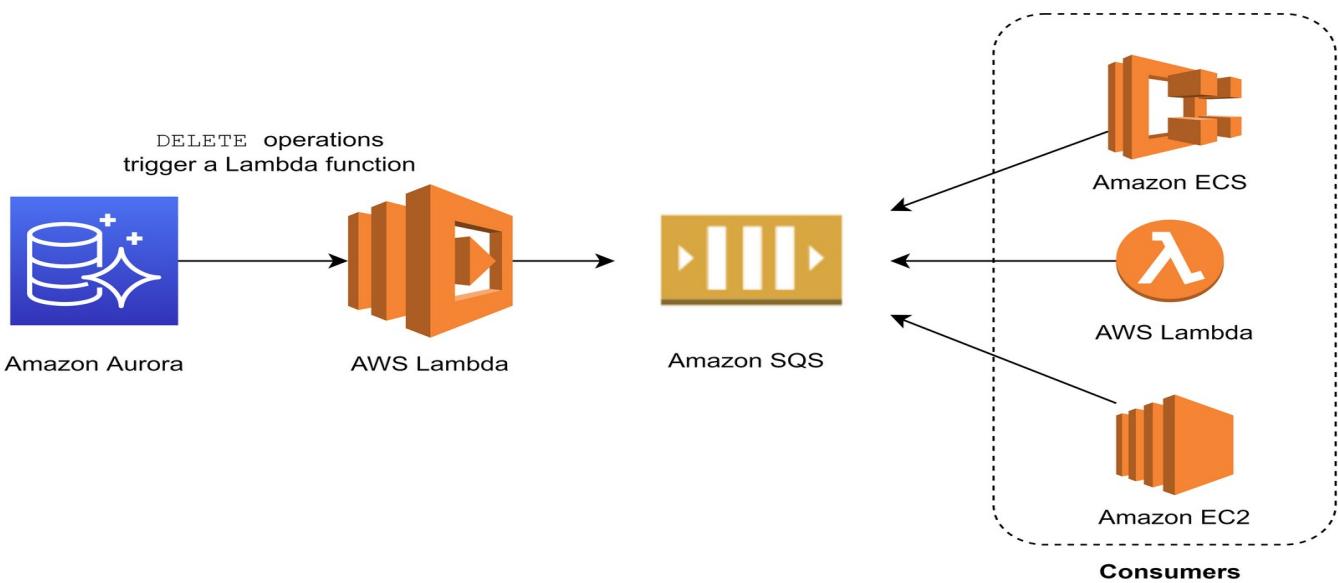
11. PERGUNTA

Categoria: CSAA - Design de Arquiteturas de Alto Desempenho

Um site de concessionária de veículos hospedado no Amazon EC2 armazena anúncios de carros em um banco de dados do Amazon Aurora gerenciado pelo Amazon RDS. Após a venda de um veículo, seus dados devem ser removidos dos anúncios atuais e encaminhados para um sistema de processamento distribuído. Qual das seguintes opções pode satisfazer o requisito fornecido?

Crie uma função nativa ou um procedimento armazenado que invoque uma função do AWS Lambda. Configure a função do Lambda para enviar notificações de eventos a uma fila do Amazon SQS para o sistema de processamento consumir.

Você pode invocar uma função do AWS Lambda a partir de um cluster de banco de dados compatível com o Amazon Aurora MySQL Edition com uma função nativa ou um procedimento armazenado. Essa abordagem pode ser útil quando você deseja integrar seu banco de dados em execução no Aurora MySQL com outros serviços da AWS. Por exemplo, você pode querer capturar alterações de dados sempre que uma linha de uma tabela for modificada no seu banco de dados.



No cenário, você pode acionar uma função Lambda sempre que uma listagem for excluída do banco de dados. Você pode então escrever a lógica da função para enviar os dados da listagem para uma fila do SQS e fazer com que diferentes processos os consumam.

Portanto, a resposta correta é: **Crie uma função nativa ou um procedimento armazenado que invoque uma função do AWS Lambda. Configure a função do Lambda para enviar notificações de eventos a uma fila do Amazon SQS para o sistema de processamento consumir.**

A opção que diz: **Criar uma assinatura de evento RDS e enviar as notificações para o Amazon SQS. Configurar as filas do SQS para distribuir as notificações de eventos para vários tópicos do Amazon SNS. Processar os dados usando funções do AWS Lambda** está incorreta porque as assinaturas de evento RDS normalmente notificam sobre alterações operacionais em vez de modificações de dados. Este método não captura modificações no banco de dados como `INSERT`, `DELETE`, ou `UPDATE`.

A opção que diz: **Criar uma assinatura de evento RDS e enviar as notificações para o AWS Lambda. Configurar a função Lambda para distribuir as notificações de eventos para várias filas do Amazon SQS para atualizar o sistema de processamento** está incorreta porque as assinaturas de evento RDS se concentram principalmente em alterações no nível operacional, em vez de capturar modificações diretas de dados.

A opção que diz: **Criar uma assinatura de evento RDS e enviar as notificações para o Amazon SNS. Configurar o tópico SNS para distribuir as notificações de eventos para várias filas do Amazon SQS. Processar os dados usando funções do AWS Lambda** está incorreta porque as assinaturas de evento RDS rastreiam apenas eventos relacionados à infraestrutura e não alterações reais no banco de dados.

Referências:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html>

<https://aws.amazon.com/blogs/database/capturando-alterações-de-dados-na-amazon-aurora-usando-aws-lambda/>

Confira esta folha de dicas do Amazon Aurora:

<https://tutorialsdojo.com/amazon-aurora/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Automatize a remoção de dados após a venda do veículo
- Encaminhe essas informações para um sistema de processamento distribuído
- Utilize recursos gerenciados e integrados da AWS
- Garanta desacoplamento e escalabilidade do processamento

A combinação de procedimentos armazenados no Aurora com AWS Lambda e Amazon SQS:

- Permite que o banco de dados dispare eventos para ações externas
- Lambda atua como intermediário para processar e encaminhar dados
- SQS desacopla o envio e o consumo das mensagens, garantindo alta disponibilidade e tolerância a falhas
- Facilita o processamento assíncrono e escalável dos dados do veículo vendido

Resumo Final:

Integrar procedimentos armazenados no banco Aurora com funções Lambda e filas SQS oferece uma solução eficiente, escalável e desacoplada para mover dados entre o banco e o sistema de processamento distribuído. Essa arquitetura garante automação, resiliência e flexibilidade, atendendo com eficácia o requisito do negócio.

12. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Um aplicativo que registra dados meteorológicos a cada minuto é implantado em uma frota de instâncias Spot do Amazon EC2 e utiliza uma instância de banco de dados MySQL RDS. Atualmente, há apenas uma instância do Amazon RDS em execução em uma Zona de Disponibilidade. O banco de dados precisa ser aprimorado para garantir alta disponibilidade, permitindo a replicação síncrona de dados para outra instância RDS.

Qual das seguintes opções executa replicação síncrona de dados no RDS?

Instância do RDS DB em execução como uma implantação Multi-AZ

Ao criar ou modificar sua instância de banco de dados para ser executada como uma implantação Multi-AZ, o Amazon RDS provisiona e mantém automaticamente uma réplica **de standby** síncrona em uma Zona de Disponibilidade diferente. As atualizações da sua instância de banco de dados são replicadas de forma síncrona entre as Zonas de Disponibilidade para o standby, a fim de manter ambas sincronizadas e proteger as atualizações mais recentes do seu banco de dados contra falhas na instância de banco de dados.

Multi-AZ Deployments	Read Replicas
Synchronous replication – highly durable	Asynchronous replication – highly scalable
Only database engine on primary instance is active	All read replicas are accessible and can be used for read scaling
Automated backups are taken from standby	No backups configured by default
Always span two Availability Zones within a single Region	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Database engine version upgrades happen on primary	Database engine version upgrade is independent from source instance
Automatic failover to standby when a problem is detected	Can be manually promoted to a standalone database instance

Portanto, a resposta correta é: **instância do RDS DB em execução como uma implantação Multi-AZ**

A réplica de leitura do RDS está incorreta, pois uma réplica de leitura fornece principalmente uma replicação assíncrona em vez de síncrona.

A Réplica de Leitura do Amazon DynamoDB está incorreta, pois não oferece o recurso de Réplica de Leitura. Normalmente, ela usa tabelas globais para replicar dados em várias regiões da AWS.

O Amazon CloudFront em execução como uma implantação Multi-AZ é , pois também não possui um recurso de Réplica de Leitura. Ele simplesmente armazena o conteúdo em cache em locais de borda, em vez de replicar os dados no banco de dados.

Referências:

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/rds/features/multi-az/>

Confira esta folha de dicas do Amazon RDS:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Garanta **alta disponibilidade** do banco de dados
- Utilize **replicação síncrona** para minimizar perda de dados
- Proporcione tolerância a falhas na Zona de Disponibilidade

A implantação Multi-AZ do Amazon RDS:

- Cria uma réplica síncrona em outra Zona de Disponibilidade

- Garante failover automático e transparente em caso de falha
- Minimiza perda de dados por replicação síncrona
- É uma solução gerenciada, sem necessidade de configuração manual da replicação
- Oferece alta disponibilidade sem complexidade operacional adicional

Resumo Final:

Para garantir alta disponibilidade e replicação síncrona em um banco de dados MySQL RDS, a configuração Multi-AZ é a melhor opção. Ela oferece failover automático e reduz o risco de perda de dados, atendendo aos requisitos críticos de sistemas com gravações frequentes e que demandam continuidade operacional.

13. PERGUNTA

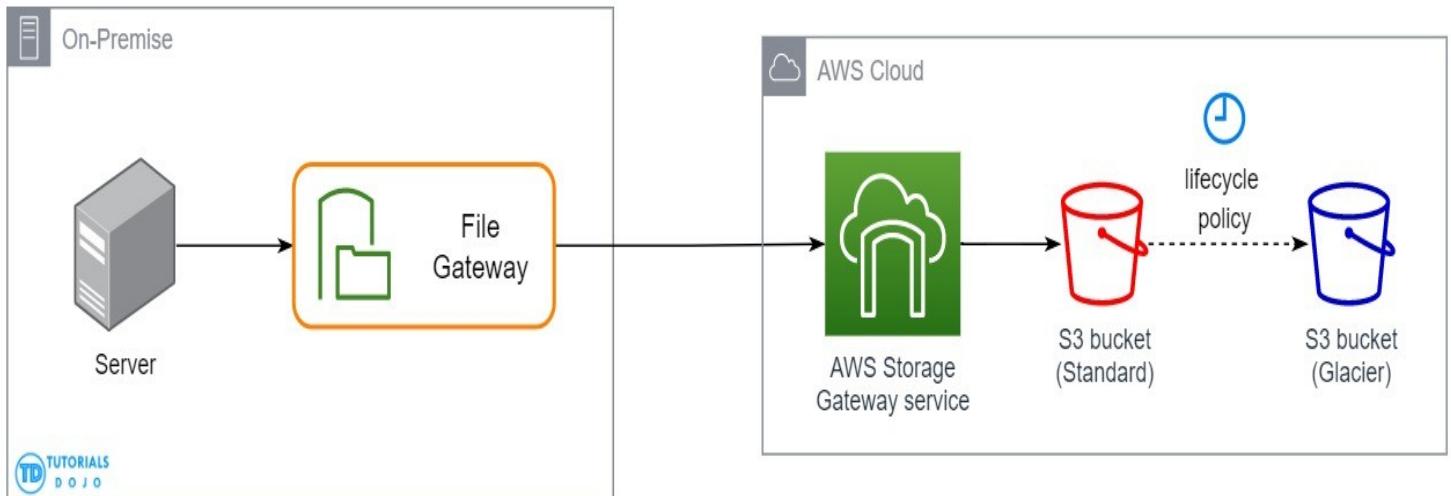
Categoria: CSAA - Design de Arquiteturas Resilientes

Uma empresa possui uma arquitetura de nuvem híbrida que conecta seu data center local e a infraestrutura de nuvem na AWS. Ela requer um backup de armazenamento durável para seus documentos corporativos armazenados localmente e um cache local que forneça acesso de baixa latência aos dados acessados recentemente para reduzir as taxas de saída de dados. Os documentos devem ser armazenados e recuperados da AWS por meio do protocolo Server Message Block (SMB). Esses arquivos devem estar acessíveis imediatamente em minutos por seis meses e arquivados por mais uma década para atender à conformidade de dados.

Qual das seguintes opções é a melhor e mais econômica abordagem para implementar neste cenário?

Inicie um novo gateway de arquivos que se conecte ao seu data center local usando o AWS Storage Gateway. Carregue os documentos no gateway de arquivos e configure uma política de ciclo de vida para mover os dados para o Glacier para arquivamento.

Um gateway de arquivos oferece suporte a uma interface de arquivos no Amazon Simple Storage Service (Amazon S3) e combina um serviço e um dispositivo de software virtual. Usando essa combinação, você pode armazenar e recuperar objetos no Amazon S3 usando protocolos de arquivo padrão do setor, como Network File System (NFS) e Server Message Block (SMB). O dispositivo de software, ou gateway, é implantado em seu ambiente local como uma máquina virtual (VM) executada no VMware ESXi, Microsoft Hyper-V ou no hipervisor Linux Kernel-based Virtual Machine (KVM).



O gateway fornece acesso a objetos no S3 como arquivos ou pontos de montagem de compartilhamento de arquivos. Com um gateway de arquivos, você pode fazer o seguinte:

- Você pode armazenar e recuperar arquivos diretamente usando o protocolo NFS versão 3 ou 4.1.

- Você pode armazenar e recuperar arquivos diretamente usando o protocolo do sistema de arquivos SMB versão 2 e 3.
- Você pode acessar seus dados diretamente no Amazon S3 a partir de qualquer aplicativo ou serviço da Nuvem AWS.
- Você pode gerenciar seus dados do Amazon S3 usando políticas de ciclo de vida, replicação entre regiões e controle de versão. Pense em um gateway de arquivos como uma montagem de sistema de arquivos no S3.

O AWS Storage Gateway oferece suporte às classes de armazenamento Amazon S3 Standard, Amazon S3 Standard - Acesso Infrequente, Amazon S3 One Zone - Acesso Infrequente e Amazon Glacier. Ao criar ou atualizar um compartilhamento de arquivos, você tem a opção de selecionar uma classe de armazenamento para seus objetos. Você pode escolher o Amazon S3 Standard ou qualquer uma das classes de armazenamento de acesso infrequente, como S3 Standard IA ou S3 One Zone IA. Objetos armazenados em qualquer uma dessas classes de armazenamento podem ser transferidos para o Amazon Glacier usando uma Política de Ciclo de Vida.

Embora você possa gravar objetos diretamente de um compartilhamento de arquivos na classe de armazenamento S3-Standard-IA ou S3-One Zone-IA, é recomendável usar uma Política de Ciclo de Vida para fazer a transição dos seus objetos em vez de gravar diretamente do compartilhamento de arquivos, especialmente se você espera atualizar ou excluir o objeto dentro de 30 dias após arquivá-lo.

Portanto, a resposta correta é: **Inicie um novo gateway de arquivos que se conecte ao seu data center local usando o AWS Storage Gateway. Carregue os documentos no gateway de arquivos e configure uma política de ciclo de vida para mover os dados para o Glacier para arquivamento.**

A opção que diz: **Inicie um novo gateway de fita que se conecte ao seu data center local usando o AWS Storage Gateway. Carregue os documentos para o gateway de fita e configure uma política de ciclo de vida para mover os dados para o Glacier para arquivamento** está incorreta porque, embora os gateways de fita forneçam dados de backup de arquivo duráveis e econômicos no Amazon Glacier, eles não atendem aos critérios de recuperação imediata em minutos. Eles também não mantêm um cache local que forneça acesso de baixa latência aos dados acessados recentemente e reduza as taxas de saída de dados. Portanto, ainda é melhor configurar um gateway de arquivo.

A opção que diz: **Estabeleça uma conexão Direct Connect para integrar sua rede local à sua VPC. Carregue os documentos no Amazon EBS Volumes e use uma política de ciclo de vida para mover automaticamente os snapshots do EBS para um bucket do Amazon S3 e, posteriormente, para o Glacier para arquivamento** está incorreta, pois os volumes do EBS não são apenas menos duráveis em comparação com o S3, como também seria mais econômico armazenar os documentos diretamente em um bucket do S3. Uma solução alternativa é usar o AWS Direct Connect com o AWS Storage Gateway para criar uma conexão para necessidades de carga de trabalho de alto rendimento, fornecendo uma conexão de rede dedicada entre seu gateway de arquivos local e a AWS. No entanto, essa solução usa o EBS e, portanto, essa opção ainda está incorreta.

A opção que diz: **Usar o AWS DataSync para transferir todos os arquivos da rede local diretamente para um bucket do Amazon S3 e configurar uma política de ciclo de vida para mover os dados para o Glacier para arquivamento** está incorreta porque o DataSync é principalmente um serviço de migração de dados que facilita transferências em massa, mas não oferece cache local para acesso de baixa latência a arquivos acessados recentemente. Sem o cache, a empresa pode incorrer em tarifas mais altas de saída de dados, tornando essa opção menos econômica.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

JUSTIFICATIVA:

A PERGUNTA EXIGE UMA SOLUÇÃO QUE:

- Atenda um ambiente híbrido (local + AWS)
- Ofereça um cache local para acesso de baixa latência a dados recentes
- Suporte o protocolo SMB para armazenamento e recuperação de arquivos
- Garanta armazenamento durável com arquivamento a longo prazo (mais de 10 anos)
- Seja a opção mais econômica para esses requisitos

O AWS Storage Gateway - File Gateway:

- Suporta protocolo SMB para integração transparente com aplicações locais
- Mantém um cache local para reduzir latência e custos de saída de dados
- Integra-se com Amazon S3, permitindo o uso de políticas de ciclo de vida para migrar dados para Glacier
- Oferece durabilidade e conformidade para arquivamento de longo prazo
- É uma solução gerenciada, econômica e escalável para armazenamento híbrido

Resumo Final:

O AWS Storage Gateway File Gateway é a solução ideal para cenários híbridos que demandam acesso local rápido via SMB, armazenamento durável na AWS e arquivamento econômico a longo prazo com o Amazon S3 Glacier. Ele combina desempenho, integração transparente e redução de custos, atendendo aos requisitos de conformidade e eficiência da empresa.

14. PERGUNTA

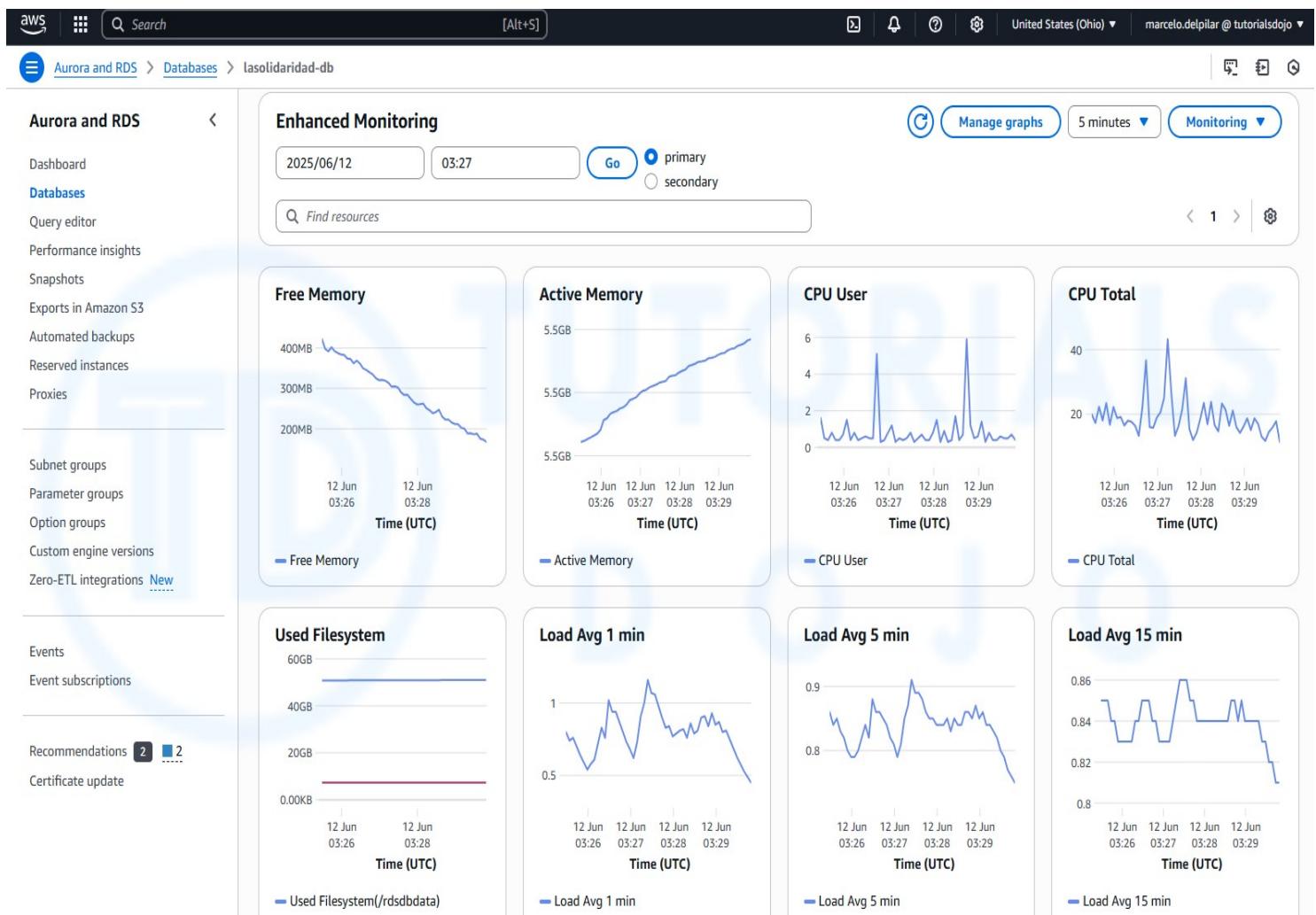
Categoria: CSAA – Design de Arquiteturas Resilientes

Uma plataforma de câmbio de criptomoedas online está hospedada na AWS, utilizando um cluster Amazon ECS e o Amazon RDS em uma configuração de implantações Multi-AZ. O aplicativo utiliza intensamente a instância RDS para processar operações complexas de leitura e gravação em banco de dados. Para manter a confiabilidade, a disponibilidade e o desempenho, é necessário monitorar de perto como os diferentes processos ou threads em uma instância de banco de dados usam a CPU, incluindo a porcentagem de largura de banda da CPU e a memória total consumida por cada processo.

Qual das seguintes opções é a solução mais adequada para monitorar o banco de dados adequadamente?

Habilitar monitoramento aprimorado no RDS.

O Amazon RDS oferece um recurso poderoso conhecido como **Monitoramento Avançado**, que fornece métricas detalhadas em tempo real sobre o sistema operacional (SO) subjacente às suas instâncias de banco de dados. Esse recurso permite que os usuários monitorem o desempenho em um nível granular por meio do Console de Gerenciamento da AWS ou acessando a saída JSON do Monitoramento Avançado por meio do CloudWatch Logs. Por padrão, essas métricas são retidas no CloudWatch Logs por 30 dias, mas esse período de retenção pode ser ajustado modificando as configurações de retenção do **RDSOSMetrics** grupo de logs no CloudWatch.



O Monitoramento Avançado difere das métricas padrão do CloudWatch, pois coleta dados diretamente de um agente instalado na instância, em vez do hipervisor, que é usado pelo CloudWatch. Essa distinção pode levar a pequenas variações entre os dois conjuntos de métricas. Por exemplo, o CloudWatch fornece métricas de utilização da CPU com base na visualização do hipervisor, enquanto o Monitoramento Avançado captura insights detalhados da própria instância, oferecendo uma representação mais precisa do uso de recursos no nível do sistema operacional.

Esse recurso é particularmente benéfico para usuários que precisam de visibilidade detalhada de como processos ou threads individuais em uma instância de banco de dados utilizam os recursos da CPU. As diferenças nos dados métricos podem se tornar mais pronunciadas ao usar classes de instância menores, já que várias máquinas virtuais são frequentemente gerenciadas pelo mesmo hipervisor, afetando a precisão das métricas baseadas no hipervisor.

Portanto, a resposta correta é: **Habilitar monitoramento aprimorado no RDS.**

A opção que diz: **Usar o Amazon CloudWatch para monitorar a utilização da CPU do seu banco de dados** está incorreta. Embora você possa usar isso para monitorar a utilização da CPU da sua instância de banco de dados, ele não fornece a porcentagem da largura de banda da CPU e a memória total consumida por cada processo do banco de dados na sua instância do RDS. Observe que o CloudWatch coleta principalmente métricas sobre a utilização da CPU do hipervisor para uma instância de banco de dados, enquanto o RDS Enhanced Monitoring coleta suas métricas de um agente na instância.

A opção que diz: **Criar um script que coleta e publica métricas personalizadas no Amazon CloudWatch, que rastreia a utilização da CPU em tempo real da instância do RDS e, em seguida, configura um painel personalizado do CloudWatch para visualizar as métricas** está incorreta. Embora seja possível usar o Amazon CloudWatch Logs e o painel do CloudWatch para monitorar a utilização da CPU da instância do banco de dados, usar apenas o CloudWatch não é suficiente para obter a porcentagem específica da largura de banda da CPU e a memória total consumida por cada processo do banco de dados. Os dados fornecidos pelo CloudWatch não são tão detalhados quanto os do recurso de monitoramento aprimorado do RDS. Observe também que você não tem acesso direto às instâncias/servidores da sua instância do banco

de dados RDS, diferentemente das suas instâncias do EC2, onde você pode instalar um agente do CloudWatch ou um script personalizado para obter a utilização da CPU e da memória da sua instância.

A opção que diz: **Verifique as métricas CPU% e MEM% que estão prontamente disponíveis no console do RDS, que mostram a porcentagem da largura de banda da CPU e a memória total consumida por cada processo de banco de dados da sua instância do RDS**, está incorreta porque as métricas de CPU% e MEM% não estão prontamente disponíveis no console do Amazon RDS, o que é contrário ao que está sendo declarado nesta opção.

Referências:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Monitoring.OS.html#USER_Monitoring.OS.CloudWatchLogs

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch>

Confira estas folhas de dicas do Amazon CloudWatch e do Amazon RDS:

<https://tutorialsdojo.com/amazon-cloudwatch/>

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

15. PERGUNTA

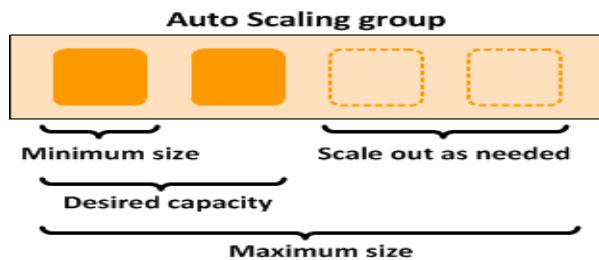
Categoria: CSAA - Design de Arquiteturas Resilientes

Uma empresa precisa implantar pelo menos duas instâncias do Amazon EC2 para suportar as cargas de trabalho normais de sua aplicação e escalar automaticamente até seis instâncias do EC2 para lidar com o pico de carga. A arquitetura deve ser altamente disponível e tolerante a falhas, pois processa cargas de trabalho de missão crítica.

Como arquiteto de soluções, o que deve ser feito para atender a esse requisito?

Crie um grupo de dimensionamento automático de instâncias do EC2 e defina a capacidade mínima como 4 e a capacidade máxima como 6. Implante 2 instâncias na Zona de Disponibilidade A e outras 2 instâncias na Zona de Disponibilidade B.

O Amazon EC2 Auto Scaling ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga do seu aplicativo. Você cria coleções de instâncias do EC2, chamadas de grupos de Auto Scaling. Você pode especificar o número mínimo de instâncias em cada grupo de Auto Scaling, e o Amazon EC2 Auto Scaling garante que seu grupo nunca fique abaixo desse tamanho. Você também pode especificar o número máximo de instâncias em cada grupo de Auto Scaling, e o Amazon EC2 Auto Scaling garante que seu grupo nunca fique acima desse tamanho.



Para obter uma arquitetura altamente disponível e tolerante a falhas para seus aplicativos, você deve implantar todas as suas instâncias em diferentes Zonas de Disponibilidade. Isso ajudará a isolar seus recursos em caso de interrupção. Observe que, para atingir a tolerância a falhas, você precisa ter recursos redundantes para evitar qualquer degradação do sistema em caso de falha do servidor ou interrupção da Zona de Disponibilidade. Ter uma arquitetura tolerante a falhas acarreta um custo extra na execução de recursos adicionais ao normalmente necessário. Isso garante que as cargas de trabalho de missão crítica sejam processadas.

Como o cenário requer pelo menos 2 instâncias para lidar com o tráfego regular, você deve ter 2 instâncias em execução o tempo todo, mesmo que ocorra uma indisponibilidade de uma AZ. Você pode usar um Grupo de Dimensionamento Automático para dimensionar automaticamente seus recursos de computação em duas ou mais Zonas de Disponibilidade. Você precisa especificar a capacidade mínima para 4 instâncias

e a capacidade máxima para 6 instâncias. Se cada AZ tiver 2 instâncias em execução, mesmo que uma delas falhe, seu sistema ainda executará no mínimo 2 instâncias.

Portanto, a resposta correta é: **Crie um grupo de dimensionamento automático de instâncias do EC2 e defina a capacidade mínima como 4 e a capacidade máxima como 6. Implante 2 instâncias na Zona de disponibilidade A e outras 2 instâncias na Zona de disponibilidade B.**

A opção que diz: **Criar um grupo de Dimensionamento Automático de instâncias EC2 e definir a capacidade mínima como 2 e a máxima como 6. Implantar 4 instâncias na Zona de Disponibilidade A** está incorreta porque as instâncias são implantadas apenas em uma única Zona de Disponibilidade. Ela não pode proteger seus aplicativos e dados contra falhas no datacenter ou na AZ.

A opção que diz: **Criar um grupo de Dimensionamento Automático de instâncias do EC2 e definir a capacidade mínima como 2 e a máxima como 6. Usar 2 Zonas de Disponibilidade e implantar 1 instância para cada AZ** está incorreta. É necessário ter 2 instâncias em execução o tempo todo. Se ocorrer uma interrupção de AZ, o ASG iniciará uma nova instância na AZ não afetada. Esse provisionamento não ocorre instantaneamente, o que significa que, por um determinado período, haverá apenas 1 instância em execução.

A opção que diz: **Criar um grupo de instâncias EC2 de Auto Scaling e definir a capacidade mínima como 2 e a máxima como 4. Implantar 2 instâncias na Zona de Disponibilidade A e 2 instâncias na Zona de Disponibilidade B** está incorreta. Embora isso atenda ao requisito de pelo menos 2 instâncias EC2 e alta disponibilidade, a configuração de capacidade máxima está incorreta. Ela deve ser definida como 6 para lidar adequadamente com o pico de carga. Se ocorrer uma interrupção na AZ e o sistema estiver em seu pico de carga, o número de instâncias em execução nessa configuração será de apenas 4, em vez de 6, e isso afetará o desempenho do seu aplicativo.

Referências:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html>

<https://docs.aws.amazon.com/documentdb/latest/developerguide/regions-and-azs.html>

Confira esta folha de dicas de dimensionamento automático da AWS:

<https://tutorialsdojo.com/aws-auto-scaling/>

16. PREGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

A empresa de tecnologia para a qual você trabalha realizou uma análise de Custo Total de Propriedade (TCO) avaliando o uso do Amazon S3 em comparação com a aquisição de mais hardware de armazenamento. O resultado foi que todos os 1.200 funcionários teriam acesso ao Amazon S3 para armazenar seus documentos pessoais.

Qual das opções a seguir você precisará considerar para poder configurar uma solução que incorpore um recurso de logon único do seu diretório corporativo do AD ou LDAP e também restrinja o acesso de cada usuário individual a uma pasta de usuário designada em um bucket do S3? (Selecione DUAS.)

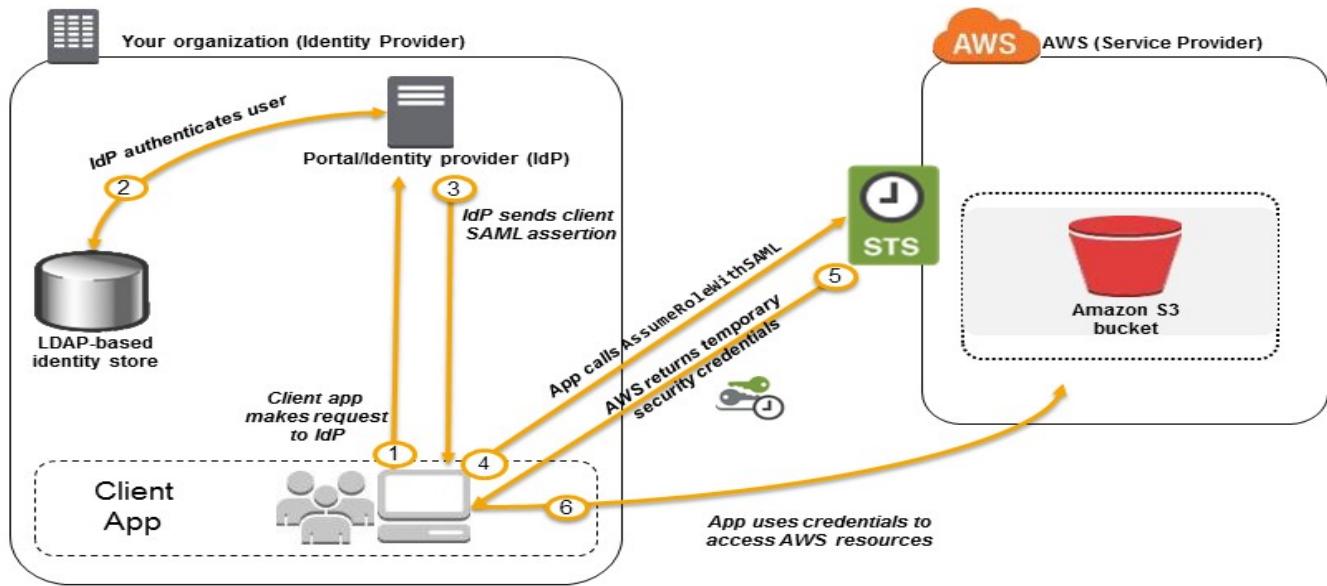
Configure uma função do IAM e uma política do IAM para acessar o bucket.

Configure um proxy de Federação ou um provedor de Identidade e use o AWS Security Token Service para gerar tokens temporários.

A pergunta se refere a um dos cenários comuns para credenciais temporárias na AWS. Credenciais temporárias são úteis em cenários que envolvem federação de identidades, delegação, acesso entre contas e funções do IAM. Neste exemplo, chama-se **federação de identidades corporativas**, considerando que você também precisa configurar um recurso de logon único (SSO).

As respostas corretas são:

- Configurar um proxy de Federação ou um provedor de Identidade e usar o AWS Security Token Service para gerar tokens temporários
- Configure uma função do IAM e uma política do IAM para acessar o bucket.



Em uma federação de identidades corporativas, você pode autenticar usuários na rede da sua organização e, em seguida, conceder a esses usuários acesso à AWS sem criar novas identidades da AWS para eles e exigir que façam login com um nome de usuário e uma senha separados. Isso é conhecido como abordagem de logon único (SSO) para acesso temporário. O AWS STS oferece suporte a padrões abertos, como o Security Assertion Markup Language (SAML) 2.0, com o qual você pode usar o Microsoft AD FS para aproveitar ao máximo o Microsoft Active Directory. Você também pode usar o SAML 2.0 para gerenciar sua própria solução de federação de identidades de usuários.

Usar soluções de login único de terceiros, como Atlassian Crowd, OKTA, OneLogin e muitas outras, é, pois você não precisa usar soluções de terceiros para fornecer o acesso. A AWS já fornece as ferramentas necessárias que você pode usar nessa situação.

Mapear cada usuário individual para uma pasta de usuário designada no S3 usando o Amazon WorkDocs para acessar seus documentos pessoais é, pois não há uma maneira direta de integrar o Amazon S3 com o Amazon WorkDocs para este cenário específico. O Amazon WorkDocs é simplesmente um serviço de criação, armazenamento e colaboração de conteúdo totalmente gerenciado e seguro. Com o Amazon WorkDocs, você pode criar, editar e compartilhar conteúdo facilmente. E como ele é armazenado centralmente na AWS, você pode acessá-lo de qualquer lugar e em qualquer dispositivo.

Configurar um usuário do IAM correspondente para cada um dos 1.200 usuários do seu diretório corporativo que precisam acessar uma pasta no bucket do S3 é, pois criar tantos usuários do IAM seria desnecessário. Além disso, você deseja que a conta seja integrada ao seu diretório do AD ou LDAP, portanto, Usuários do IAM não atende a esses critérios.

Referências:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_oidc.html

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/>

Confira esta folha de dicas do AWS IAM:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

17. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Uma empresa de e-commerce utiliza um Amazon API Gateway regional para hospedar suas APIs REST públicas. O endpoint do API Gateway é acessado por meio de um nome de domínio personalizado configurado com um registro de alias do Amazon Route 53. Para apoiar a melhoria contínua, a empresa pretende lançar uma nova versão de suas APIs com recursos aprimorados e otimizações de desempenho. Como a empresa pode reduzir a interrupção do cliente e garantir a perda MÍNIMA de dados durante o processo de atualização da maneira MAIS econômica?

Implemente uma estratégia de implantação de versão canário para o API Gateway. Implemente a versão mais recente das APIs em um estágio canário e direcione parte do tráfego de usuários para esse estágio. Verifique as novas APIs. Aumente gradualmente a porcentagem de tráfego, monitore quaisquer problemas e, se for bem-sucedido, promova o estágio canário para produção.

O Amazon API Gateway é um serviço totalmente gerenciado que facilita a criação, publicação, manutenção, monitoramento e proteção de APIs para desenvolvedores em qualquer escala. Ele funciona como uma porta de entrada para suas APIs, permitindo que você projete e implemente APIs escaláveis, altamente disponíveis e seguras. Com o Amazon API Gateway, você pode criar APIs RESTful que podem ser utilizadas por qualquer cliente HTTP, como navegadores da web e dispositivos móveis.

The screenshot shows the 'Create canary' configuration page in the AWS API Gateway console. It includes sections for 'Canary settings', 'Canary stage variables', and a summary table. The 'Canary settings' section shows a distribution of 0% to the canary and 100% to the current stage. The 'Canary stage variables' section shows a variable named 'stageName' with a value of 'Canary test'. The summary table shows the total traffic distribution across three stages: 'Canary' at 0%, 'Current stage' at 100%, and 'Stage A' at 0%. The bottom right corner features the TUTORIALS DO JOO logo.

Create canary

Canary settings

A canary is used to test new API deployments and/or changes to stage variables. A canary can receive a percentage of requests going to your stage. In addition, API deployments will be made to the canary first before being able to be promoted to the entire stage.

Request distribution

Enter the percentage of API traffic that will be diverted to the canary. The remainder will be sent to the current stage.

Canary	Current stage
0%	100%

Stage cache

Enable stage cache to store responses and use cached entries to return results to the next canary requests.

Canary stage variables

By default, your canary inherits stage variables from the stage. You can override these stage variables or add new ones. When promoting a Canary's settings to the stage, the stage is able to update its stage variables to reflect any overridden values and includes any new stage variables created by the canary.

Name	Stage value	Canary override
stageName	Canary test	

Add stage variable

Implementar uma estratégia de implantação de lançamento canário para o API Gateway é uma ótima maneira de garantir que suas APIs permaneçam estáveis e confiáveis. Essa estratégia envolve o lançamento de uma nova versão da sua API para um pequeno subconjunto de usuários, permitindo que você teste a versão mais recente em um ambiente controlado.

Se a nova versão apresentar bom desempenho, você poderá implementar a atualização gradualmente para os demais usuários. Essa abordagem permite detectar quaisquer problemas antes que afetem toda a sua base de usuários, minimizando o impacto sobre os clientes. Ao usar o Amazon API Gateway, você pode implementar rapidamente uma estratégia de implantação de versão canário, garantindo que suas APIs estejam sempre atualizadas e com o melhor desempenho.

Portanto, a resposta correta é: **implementar uma estratégia de implantação de versão canário para o API Gateway. Implantar a versão mais recente das APIs em um estágio canário e direcionar parte do tráfego de usuários para esse estágio. Verificar as novas APIs. Aumentar gradualmente a porcentagem de tráfego, monitorar quaisquer problemas e, se bem-sucedido, promover o estágio canário para produção.**

A opção que diz: **Criar um novo API Gateway com a versão atualizada das APIs no formato de arquivo OpenAPI JSON ou YAML, mas manter o mesmo nome de domínio personalizado para o novo API Gateway** está incorreta. Atualizar para um novo API Gateway usando uma versão atualizada das APIs no formato de

arquivo OpenAPI JSON ou YAML, mantendo o mesmo nome de domínio personalizado, normalmente pode resultar em tempo de inatividade e confusão durante a migração. Isso ocorre devido a atrasos na propagação do DNS, que podem afetar negativamente os usuários e até mesmo levar à perda de dados.

A opção que diz: **Modificar o API Gateway existente com a versão atualizada das APIs, mas manter o mesmo nome de domínio personalizado para o novo API Gateway usando a operação de importação para atualização no modo de substituição ou mesclagem** está incorreta. Usar a operação de importação para atualização no modo de substituição ou mesclagem pode não fornecer isolamento e testes de controle suficientes para a nova versão das APIs. Se algo der errado durante o processo de atualização, isso poderá levar à perda de dados no API Gateway existente, potencialmente afetando todos os clientes simultaneamente.

A opção que diz: **Implementar uma estratégia de implantação azul-verde para o API Gateway, implantando a versão mais recente das APIs no ambiente verde. Rotear parte do tráfego de usuários para ele, validar as novas APIs e, uma vez completamente validadas, promover o ambiente verde para produção** está incorreta. Em uma implantação azul-verde, os ambientes azul (existente) e verde (atualizado) devem ser provisionados e mantidos. Isso adiciona complexidade e custo ao processo de atualização, o que viola o requisito de custo explicitamente mencionado no cenário. Além disso, direcionar parte do tráfego de usuários para o ambiente verde pode causar problemas para esses usuários, especialmente se houver bugs não descobertos ou problemas de desempenho nas APIs atualizadas.

Referências:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html>

<https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html>

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-import-api-update.html>

Confira esta folha de dicas do Amazon API Gateway:

<https://tutorialsdojo.com/amazon-api-gateway/>

18. PERGUNTA

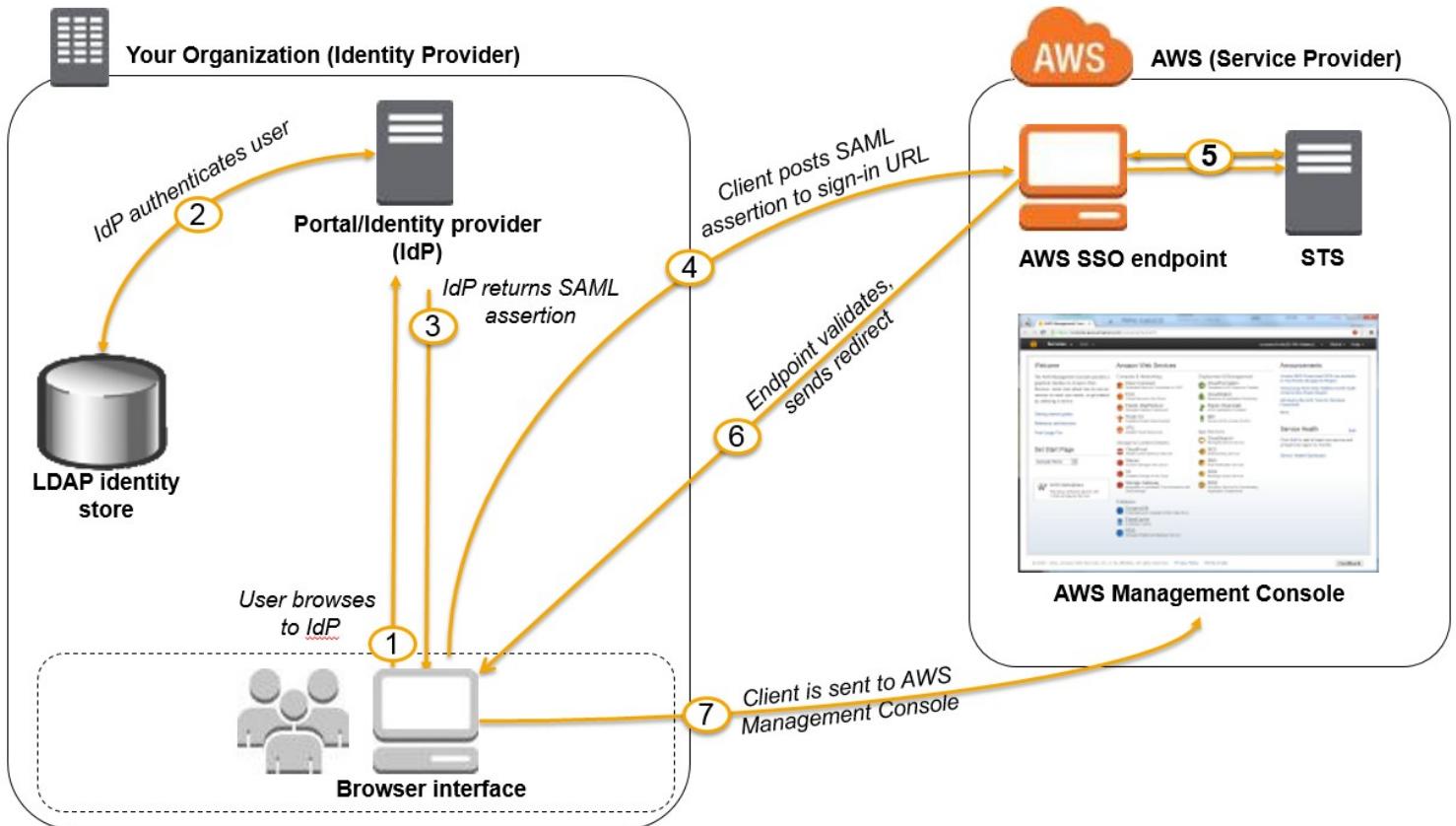
Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa farmacêutica possui recursos hospedados em sua rede local e na nuvem da AWS. A empresa exige que todos os Arquitetos de Software acessem os recursos em ambos os ambientes usando credenciais locais, armazenadas no Active Directory.

Nesse cenário, qual das seguintes opções pode ser usada para atender a esse requisito?

Configure a Federação Baseada em SAML 2.0 usando um Serviço de Federação do Microsoft Active Directory.

Como a empresa utiliza o Microsoft Active Directory, que implementa a Linguagem de Marcação para Asserção de Segurança (SAML), você pode configurar uma Federação Baseada em SAML para acesso à API da sua nuvem AWS. Dessa forma, você pode se conectar facilmente à AWS usando as credenciais de login da sua rede local.



A AWS oferece suporte à federação de identidades com SAML 2.0, um padrão aberto usado por muitos provedores de identidade (IdPs). Esse recurso permite o logon único (SSO) federado, permitindo que os usuários façam login no Console de Gerenciamento da AWS ou chamem as APIs da AWS sem a necessidade de criar um usuário do IAM para todos na sua organização. Ao usar SAML, você simplifica o processo de configuração da federação com a AWS, pois pode usar o serviço do IdP em vez de escrever um código de proxy de identidade personalizado.

Antes de usar a federação baseada em SAML 2.0, conforme descrito no cenário e diagrama anteriores, você precisa configurar o IdP da sua organização e sua conta da AWS para que confiem um no outro. O processo geral para configurar essa confiança é descrito nas etapas a seguir. Dentro da sua organização, você precisa ter um IdP compatível com SAML 2.0, como o Serviço de Federação do Microsoft Active Directory (AD FS, parte do Windows Server), o Shibboleth ou outro provedor SAML 2.0 compatível.

Portanto, a resposta correta é: **Configurar a Federação Baseada em SAML 2.0 usando um Serviço de Federação do Microsoft Active Directory.**

A opção que diz: **Configurando a Federação Baseada em SAML 2.0 usando uma Federação de Identidade Web** está incorreta, pois é usada principalmente para permitir que os usuários façam login por meio de um provedor de identidade externo (IdP) conhecido, como Login com Amazon, Facebook e Google. Ela não utiliza o Active Directory.

A opção que diz: **Usar usuários do IAM** está incorreta porque a situação exige que você use as credenciais existentes armazenadas no Active Directory, e não as contas de usuário que serão geradas pelo IAM.

A opção que diz: **Usando a Amazon VPC** está incorreta porque isso só permite provisionar uma seção logicamente isolada da Nuvem AWS, onde você pode iniciar recursos da AWS em uma rede virtual definida por você. Isso não tem nada a ver com autenticação de usuário ou com o Active Directory.

Referências:

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

Confira esta folha de dicas do AWS IAM:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

19. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa está projetando um portal bancário que utiliza o Amazon ElastiCache para Redis como componente de gerenciamento de sessão distribuída. Para proteger os dados da sessão e garantir que os engenheiros de nuvem se autentiquem antes de executar comandos do Redis, especificamente **MULTI EXEC** comandos, o sistema deve impor uma autenticação forte, exigindo que os usuários insiram uma senha. Além disso, o acesso deve ser gerenciado com credenciais de longa duração, além de oferecer suporte a práticas de segurança robustas.

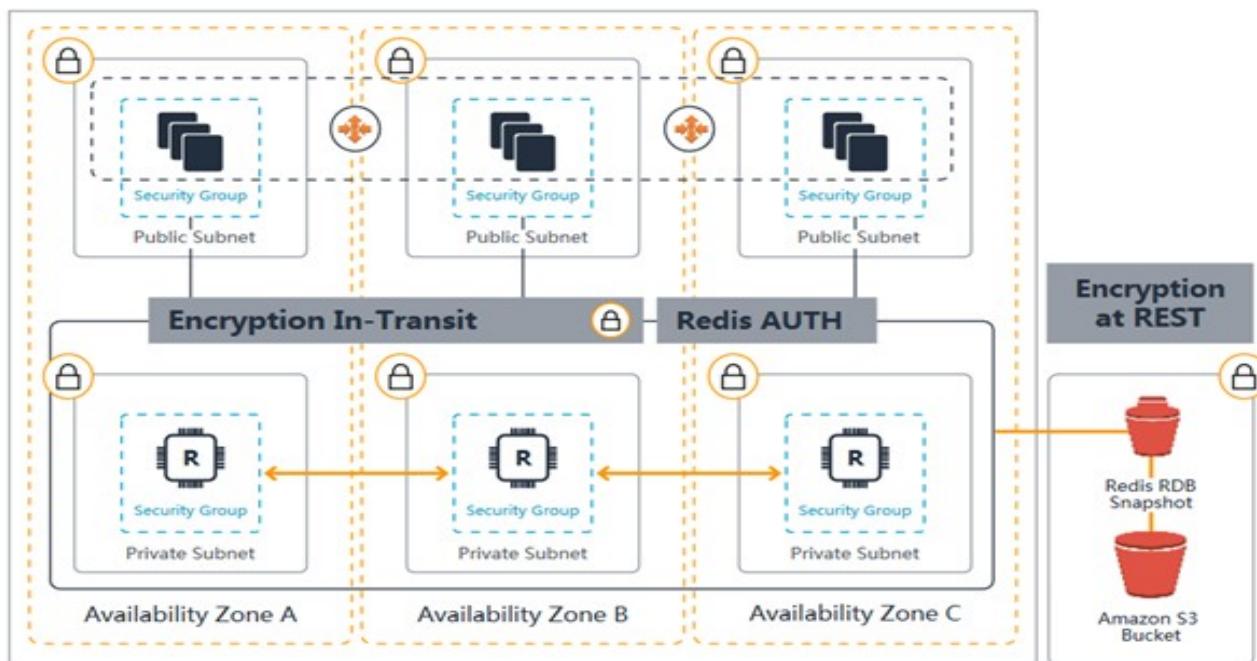
Qual das seguintes ações deve ser tomada para atender ao requisito acima?

Autentique os usuários usando o Redis AUTH criando um novo Redis Cluster com os parâmetros **--transit-encryption-enabled** e **--auth-token** habilitados.

Usar o comando **RedisAUTH** pode melhorar a segurança dos dados exigindo que o usuário insira uma senha antes de receber permissão para executar comandos Redis em um servidor Redis protegido por senha.

Portanto, a resposta correta é: **Autentique os usuários usando o Redis AUTH criando um novo Redis Cluster com os parâmetros --transit-encryption-enabled e --auth-token habilitados.**

Para exigir que os usuários insiram uma senha em um servidor Redis protegido por senha, inclua o parâmetro **--auth-token** com a senha correta ao criar seu grupo de replicação ou cluster e em todos os comandos subsequentes para o grupo de replicação ou cluster.



A opção que diz: **Gerar um token de autenticação do IAM usando credenciais da AWS e fornecer esse token como senha** está incorreta. A autenticação do IAM simplesmente não é compatível com a execução de comandos do Redis como **MULTI EXEC**, e os tokens do IAM expiram a cada 12 horas, o que não atende à necessidade de credenciais de longa duração.

A opção que diz: **Configurar um grupo de replicação do Redis e habilitar o AtRestEncryptionEnabled** parâmetro está incorreta porque o recurso Criptografia em Repouso do Redis protege apenas os dados dentro do armazenamento de dados na memória. Em vez disso, você precisa usar a opção AUTH do Redis.

A opção que diz: **Habilitar a criptografia em trânsito para grupos de replicação do Redis** está incorreta. Embora a criptografia em trânsito faça parte da solução, ela não inclui o mais importante: a opção Redis AUTH.

Referências:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html>

Confira esta folha de dicas do Amazon ElastiCache:

<https://tutorialsdojo.com/amazon-elasticsearch/>

Redis (modo cluster habilitado vs desabilitado) vs Memcached:

<https://tutorialsdojo.com/redis-cluster-mode-enabled-vs-disabled-vs-memcached/>

20. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Houve um incidente em um ambiente de produção onde dados de usuários armazenados em um bucket do Amazon S3 foram excluídos acidentalmente por um Engenheiro de DevOps Júnior. O problema foi encaminhado à gerência e, após alguns dias, foi dada uma instrução para aprimorar a segurança e a proteção dos recursos da AWS.

Qual combinação das seguintes opções protegerá os objetos do S3 no bucket contra exclusão acidental e substituição? (Selecione DUAS.)

Habilitar controle de versão

Habilitar autenticação multifator Excluir

Ao usar o controle de versão e habilitar a exclusão MFA (autenticação multifator), você pode proteger e recuperar seus objetos S3 contra exclusão acidental ou substituição.

The screenshot shows the 'Edit Bucket Versioning' page for the 'tutorialsdojo-pasig' bucket. At the top, there's a 'Bucket Versioning' section with a description of what versioning does. Below it, there are two radio button options: 'Suspend' (disabled) and 'Enable' (selected). A note below the 'Enable' option states: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' In the 'Multi-factor authentication (MFA) delete' section, it says 'Enabled'. At the bottom right, there are 'Cancel' and 'Save changes' buttons. The Tutorials Dojo logo is in the bottom left corner.

O versionamento é um meio de manter múltiplas variantes de um objeto no mesmo bucket. Buckets com versionamento habilitado permitem recuperar objetos de exclusões ou substituições acidentais. Você pode usar o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto.

armazenado no seu bucket do Amazon S3. Com o versionamento, você pode se recuperar facilmente de ações não intencionais do usuário e de falhas no aplicativo.

▼ Using the AWS CLI

The following example enables S3 Versioning and multi-factor authentication (MFA) delete on a bucket.

```
aws s3api put-bucket-versioning --bucket DOC-EXAMPLE-BUCKET1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

Você também pode adicionar opcionalmente outra camada de segurança configurando um bucket para habilitar a exclusão de MFA (autenticação multifator), que requer autenticação adicional para qualquer uma das seguintes operações:

- Alterar o estado de versionamento do seu bucket
- Excluir permanentemente uma versão do objeto

O MFA Delete requer duas formas de autenticação juntas:

- Suas credenciais de segurança
- A concatenação de um número de série válido, um espaço e o código de seis dígitos exibido em um dispositivo de autenticação aprovado.

Portanto, as respostas corretas são:

- **Habilitar controle de versão**
- **Habilitar autenticação multifator Excluir**

A opção que diz: **Fornecer acesso aos dados do S3 estritamente por meio de URL pré-assinada** está incorreta, pois uma URL pré-assinada concede acesso ao objeto identificado na URL. URLs pré-assinadas são úteis quando os clientes carregam um objeto para o seu bucket do S3, mas não ajudam a evitar exclusões acidentais.

A opção que diz: **Não permitir a exclusão do S3 usando uma política de bucket do IAM** está incorreta, pois você ainda quer que os usuários possam excluir objetos no bucket e apenas quer evitar exclusões acidentais. Não permitir a exclusão do S3 usando uma política de bucket do IAM restringirá todas as operações de exclusão ao seu bucket.

A opção que diz: **Habilitar o S3 Intelligent-Tiering** está incorreta, pois o S3 Intelligent-Tiering não ajuda nessa situação.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

21. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa de desenvolvimento de software está usando computação sem servidor com o AWS Lambda para criar e executar aplicativos sem precisar configurar ou gerenciar servidores. A empresa possui uma função Lambda que se conecta a um MongoDB Atlas, uma plataforma popular de Banco de Dados como Serviço

(DBaaS), e também utiliza uma API de terceiros para buscar determinados dados para seu aplicativo. Um dos desenvolvedores foi instruído a criar as variáveis de ambiente para o nome do host, nome de usuário e senha do banco de dados MongoDB, bem como as credenciais da API que serão usadas pela função Lambda para os ambientes DEV, SIT, UAT e PROD.

Considerando que a função Lambda armazena credenciais sensíveis de banco de dados e API, como essas informações podem ser protegidas para impedir que outros desenvolvedores da equipe, ou qualquer pessoa, vejam essas credenciais em texto simples? Selecione a melhor opção que ofereça segurança máxima.

Crie uma nova chave AWS KMS e use-a para habilitar auxiliares de criptografia que utilizam o AWS Key Management Service para armazenar e criptografar informações confidenciais.

Ao criar ou atualizar funções do Lambda que usam variáveis de ambiente, o AWS Lambda as criptografa usando o AWS Key Management Service. Quando a função do Lambda é invocada, esses valores são descriptografados e disponibilizados para o código do Lambda.

Na primeira vez que você cria ou atualiza funções do Lambda que usam variáveis de ambiente em uma região, uma chave de serviço padrão é criada automaticamente no AWS KMS. Essa chave é usada para criptografar variáveis de ambiente. No entanto, se desejar usar auxiliares de criptografia e usar o KMS para criptografar variáveis de ambiente após a criação da função do Lambda, você deverá criar sua própria chave do AWS KMS e escolhê-la em vez da chave padrão. A chave padrão apresentará erros quando escolhida. Criar sua própria chave oferece mais flexibilidade, incluindo a capacidade de criar, rotacionar, desabilitar e definir controles de acesso, além de auditar as chaves de criptografia usadas para proteger seus dados.

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#)

password	AQICAHgdCwJ7eNzG0cBk9Q6nDD21wmtlCsvWz2AsE75No	Encrypt	Code	Remove
Key	Value	Encrypt	Code	Remove

▼ Encryption configuration

Enable helpers for encryption in transit [Info](#)

AWS KMS key to encrypt in transit

arn:aws:kms:us-east-1:8420 [?key/2defc6c2-ab8a-499f-87de-](#) [X](#)

AWS KMS call failed for reason: User: arn:aws:iam::84205 7:user/koko is not authorized to perform: kms:Encrypt on resource: arn:aws:kms:us-east-1:84205 2defc6c2-ab8a-499f-87de-

AWS KMS key to encrypt at rest [Info](#)
Choose an AWS KMS key to encrypt the environment variables at rest, or simply let Lambda manage the encryption.

(default) aws/lambda
 Use a customer master key

Portanto, a resposta correta é: **crie uma nova chave AWS KMS e use-a para habilitar auxiliares de criptografia que utilizam o AWS Key Management Service para armazenar e criptografar informações confidenciais.**

A opção que diz: **Não há necessidade de fazer nada porque, por padrão, o Lambda já criptografa as variáveis de ambiente usando o AWS Key Management Service** está incorreta. Embora o Lambda criptografe as variáveis de ambiente em sua função por padrão, as informações confidenciais ainda estarão visíveis

para outros usuários que tenham acesso ao console do Lambda. Isso ocorre porque o Lambda usa uma chave KMS padrão para criptografar as variáveis, que geralmente é acessível a outros usuários. A melhor opção nesse cenário é usar auxiliares de criptografia para proteger suas variáveis de ambiente.

A opção que diz: **Habilitar criptografia SSL que utiliza o AWS CloudHSM para armazenar e criptografar informações confidenciais** também está incorreta, pois habilitar o SSL criptografaria os dados apenas em trânsito. Suas outras equipes ainda conseguiriam visualizar o texto simples em repouso. Normalmente, o AWS KMS é a opção recomendada para criptografar dados confidenciais em repouso.

A opção que diz: **O Lambda não fornece criptografia para as variáveis de ambiente. Em vez disso, implante seu código em uma instância do Amazon EC2** está incorreta, pois, como mencionado, o Lambda fornece funcionalidade de criptografia para variáveis de ambiente.

Referências:

https://docs.aws.amazon.com/lambda/latest/dg/env_variables.html#env_encrypt

https://docs.aws.amazon.com/lambda/latest/dg/tutorial-env_console.html

Confira esta folha de dicas do AWS Lambda:

<https://tutorialsdojo.com/aws-lambda/>

22. PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa de registros médicos planeja armazenar dados confidenciais de ensaios clínicos em um repositório do Amazon S3 com o recurso de versionamento em nível de objeto habilitado. O Arquiteto de Soluções tem a tarefa de garantir que nenhum objeto possa ser substituído ou excluído por qualquer usuário no período de apenas um ano. Para atender aos rigorosos requisitos de conformidade, o usuário root da conta AWS da empresa também deve ser impedido de fazer alterações em um objeto no bucket do S3.

Qual das seguintes opções é a maneira mais segura de armazenar dados no S3?

Habilite o bloqueio de objeto S3 no modo de conformidade com um período de retenção de um ano.

Com o S3 Object Lock, você pode armazenar objetos usando um modelo WORM (gravação única e leitura múltipla). O Object Lock pode ajudar a impedir que objetos sejam excluídos ou substituídos por um período fixo ou indefinidamente. Você pode usar o Object Lock para atender aos requisitos regulatórios que exigem armazenamento WORM ou simplesmente adicionar outra camada de proteção contra alterações e exclusões de objetos.

Antes de bloquear qualquer objeto, você precisa habilitar um bucket para usar o Bloqueio de Objetos do S3. Você habilita o Bloqueio de Objetos ao criar um bucket. Depois de habilitar o Bloqueio de Objetos em um bucket, você pode bloquear objetos nesse bucket. Ao criar um bucket com o Bloqueio de Objetos habilitado, você não pode desabilitar o Bloqueio de Objetos nem suspender o versionamento para esse bucket.

O S3 Object Lock fornece dois modos de retenção:

-Modo de governança

-Modo de conformidade

Esses modos de retenção aplicam diferentes níveis de proteção aos seus objetos. Você pode aplicar qualquer um dos modos de retenção a qualquer versão de objeto protegida pelo Bloqueio de Objeto.

AWS Services Search for services, features, blogs, docs, and more [Option+S]

Support Lightsail Trusted Advisor IAM AWS Budgets Amazon Macie

Amazon S3 X

Amazon S3 > Buckets > tutorialsdojo-object-lock-demo > Edit Object Lock

Edit Object Lock Info

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Once Amazon S3 Object Lock is enabled, you can't disable Object Lock or suspend Bucket Versioning for the bucket.

Object Lock
Enabled

Default retention
Automatically protect new objects put into this bucket from being deleted or overwritten.
 Disable
 Enable

Default retention mode
 Governance
Users with specific IAM permissions can overwrite or delete protected object versions during the retention period.
 Compliance
No users can overwrite or delete protected object versions during the retention period.

Default retention period
365 Days Must be a positive whole number.

Cancel **Save changes**



S3 Object Lock Retention Modes

Feedback Looking for language selection? Find it in the new Unified Settings [?](#)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

No modo de governança, os usuários não podem substituir ou excluir uma versão de objeto ou alterar suas configurações de bloqueio, a menos que tenham permissões especiais. Com o modo de governança, você protege os objetos contra exclusão pela maioria dos usuários, mas ainda pode conceder a alguns usuários permissão para alterar as configurações de retenção ou excluir o objeto, se necessário. Você também pode usar o modo de governança para testar as configurações do período de retenção antes de criar um período de retenção no modo de conformidade.

No modo de conformidade, uma versão de objeto protegida não pode ser substituída ou excluída por nenhum usuário, incluindo o usuário raiz da sua conta da AWS. Quando um objeto está bloqueado no modo de conformidade, seu modo de retenção não pode ser alterado e seu período de retenção não pode ser reduzido. O modo de conformidade ajuda a garantir que uma versão de objeto não possa ser substituída ou excluída durante o período de retenção.

Para substituir ou remover as configurações de retenção do modo de governança, um usuário deve ter `s3:BypassGovernanceRetention` permissão e deve incluir explicitamente `x-amz-bypass-governance-retention:true` como um cabeçalho de solicitação qualquer solicitação que exija a substituição do modo de governança.

Suspensão legal vs. Período de retenção



Com o Bloqueio de Objetos, você também pode aplicar uma retenção legal a uma versão de objeto. Assim como um período de retenção, uma retenção legal impede que uma versão de objeto seja substituída ou excluída. No entanto, uma retenção legal não tem um período de retenção associado e permanece em vigor até ser removida. As retenções legais podem ser aplicadas e removidas livremente por qualquer usuário que tenha `s3:PutObjectLegalHold` permissão.

As retenções legais são independentes dos períodos de retenção. Desde que o bucket que contém o objeto tenha o Bloqueio de Objeto habilitado, você pode aplicar e remover retenções legais independentemente de a versão do objeto especificada ter um período de retenção definido. Aplicar uma retenção legal a uma versão do objeto não afeta o modo ou o período de retenção dessa versão do objeto.

Por exemplo, suponha que você coloque uma retenção legal em uma versão de objeto enquanto ela também estiver protegida por um período de retenção. Se o período de retenção expirar, o objeto não perderá sua proteção contra WORM. Em vez disso, a retenção legal continuará protegendo o objeto até que um usuário autorizado a remova explicitamente. Da mesma forma, se você remover uma retenção legal enquanto uma versão de objeto estiver com um período de retenção em vigor, a versão do objeto permanecerá protegida até que o período de retenção expire.

Portanto, a resposta correta é: **Habilitar o bloqueio de objeto S3 no modo de conformidade com um período de retenção de um ano.**

A opção que diz: **Habilitar Bloqueio de Objeto S3 no modo de governança com um período de retenção de um ano** está incorreta porque, no modo de governança, os usuários normalmente não podem substituir ou excluir uma versão de objeto ou alterar suas configurações de bloqueio, a menos que tenham permissões especiais ou que um usuário tenha acesso à conta de usuário raiz da AWS. Uma opção melhor aqui é usar o modo de conformidade.

A opção que diz: **Habilitar Bloqueio de Objetos S3 no modo de governança com retenção legal de um ano** está incorreta. Não é possível definir um período para uma retenção legal. Você só pode fazer isso usando a opção "período de retenção". Observe que uma retenção legal ainda impedirá que os usuários alterem os objetos S3, mesmo após o período de retenção de um ano. Além disso, o modo de governança permitirá que o usuário root modifique seus objetos S3 e substitua quaisquer configurações existentes.

A opção que diz: **Habilitar Bloqueio de Objetos S3 no modo de conformidade com retenção legal de um ano** está incorreta. Embora a opção de usar o modo de conformidade esteja correta, você ainda não pode definir um período de um ano para a opção de retenção legal. Lembre-se de que a retenção legal é independente do período de retenção.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

23 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa possui um aplicativo web que utiliza o Amazon CloudFront para distribuir suas imagens, vídeos e outros conteúdos estáticos armazenados em seu bucket do Amazon S3 para usuários em todo o mundo. A empresa introduziu recentemente um novo recurso de acesso exclusivo para membros para alguns de seus arquivos de mídia de alta qualidade. Há um requisito para fornecer acesso a vários arquivos de mídia privados apenas para assinantes pagantes, sem a necessidade de alterar os URLs atuais. Qual das seguintes opções é a solução mais adequada para implementar para atender a esse requisito?

Use Cookies Assinados para controlar quem pode acessar os arquivos privados na sua distribuição do CloudFront, modificando seu aplicativo para determinar se um usuário deve ter acesso ao seu conteúdo. Para membros, envie os `Set-Cookie` cabeçalhos necessários ao visualizador, o que desbloqueará o conteúdo apenas para eles.

Muitas empresas que distribuem conteúdo pela internet desejam restringir o acesso a documentos, dados comerciais, fluxos de mídia ou conteúdo destinado a usuários selecionados, por exemplo, usuários que pagaram uma taxa. Para disponibilizar esse conteúdo privado com segurança usando o CloudFront, você pode fazer o seguinte:

- Exija que seus usuários acessem seu conteúdo privado usando URLs assinadas especiais do CloudFront ou cookies assinados.
- Exija que seus usuários acessem seu conteúdo usando URLs do CloudFront, não URLs que acessam o conteúdo diretamente no servidor de origem (por exemplo, Amazon S3 ou um servidor HTTP privado). Exigir URLs do CloudFront não é necessário, mas recomendamos para evitar que os usuários ignorem as restrições que você especifica em URLs assinadas ou cookies assinados.

URLs assinadas e cookies assinados do CloudFront fornecem a mesma funcionalidade básica: eles permitem que você controle quem pode acessar seu conteúdo.

The screenshot shows two sections side-by-side. On the left, under 'SIGNED URLs', there is a red icon with a white 'C' and a pen, and a blue icon with a chain and a shield. Below these icons is the text 'SIGNED URLs'. On the right, under 'CloudFront Distribution with Custom Domain Name', a URL is shown: <https://tutorialsdojo.com/report.pdf>. The URL includes several parameters: ?Expires=13570344005, &Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5EwRunQA..., and &Key-Pair-Id=K2JCJMDEHXQW5F. On the far left, there is a Tutorials Dojo logo. On the right, a screenshot of the Chrome DevTools Application tab is shown, with the 'Cookies' section expanded. It lists three cookies: '_ga', 'signed_user_cookie_1', and 'user_id'. The 'signed_user_cookie_1' cookie is highlighted with a green border. The URL https://portal.tutorialsdojo.com is also visible in the list.

Se você deseja fornecer conteúdo privado pelo CloudFront e está tentando decidir se deve usar URLs assinadas ou cookies assinados, considere o seguinte:

Use **URLs assinadas** nos seguintes casos:

- Você deseja usar uma distribuição RTMP. Cookies assinados não são suportados por distribuições RTMP.
- Você deseja restringir o acesso a arquivos individuais, por exemplo, um download de instalação do seu aplicativo.
- Seus usuários estão usando um cliente (por exemplo, um cliente HTTP personalizado) que não suporta cookies.

Utilize **cookies assinados** para os seguintes casos:

- Você deseja fornecer acesso a vários arquivos restritos, por exemplo, todos os arquivos de um vídeo no formato HLS ou todos os arquivos na área de assinantes de um site.
- Você não quer alterar seus URLs atuais.

Portanto, a resposta correta é: **Use Cookies Assinados para controlar quem pode acessar os arquivos privados na sua distribuição do CloudFront, modificando seu aplicativo para determinar se um usuário deve ter acesso ao seu conteúdo. Para membros, envie os Set-Cookie cabeçalhos necessários ao visualizador, o que desbloqueará o conteúdo apenas para eles.**

A opção que diz: **Configure sua distribuição do CloudFront para usar o Match Viewer como sua Política de Protocolo de Origem, que corresponderá automaticamente à solicitação do usuário. Isso permitirá o acesso ao conteúdo privado se a solicitação for de um membro pagante e o negará se não for um membro,** está incorreta, pois o Match Viewer é uma Política de Protocolo de Origem que configura o CloudFront para se comunicar com sua origem usando HTTP ou HTTPS, dependendo do protocolo da solicitação do visualizador. O CloudFront armazena o objeto em cache apenas uma vez, mesmo que os visualizadores façam solicitações usando os protocolos HTTP e HTTPS.

A opção que diz: **Criar uma URL Assinada com uma política personalizada que permite apenas que os membros vejam os arquivos privados** está incorreta, pois as URLs Assinadas são usadas principalmente para fornecer acesso a arquivos individuais, como mostrado na explicação acima. Além disso, o cenário diz explicitamente que eles não desejam alterar suas URLs atuais, e é por isso que implementar Cookies Assinados é mais adequado do que URLs Assinadas.

A opção que diz: **Configurar sua distribuição do CloudFront para usar a Criptografia em Nível de Campo para proteger seus dados privados e permitir acesso apenas a membros** está incorreta, pois a Criptografia em Nível de Campo permite apenas o upload seguro de informações confidenciais enviadas por usuários para seus servidores web. Ela não fornece acesso para baixar vários arquivos privados.

Referências:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

Confira esta folha de dicas do Amazon CloudFront:

<https://tutorialsdojo.com/amazon-cloudfront/>

24. PERGUNTA

Categoria: CSAA - Design de Arquiteturas Resilientes

Um conjunto de aplicações web está hospedado em um grupo de Auto Scaling de instâncias do Amazon EC2 em três Zonas de Disponibilidade e está configurado com as configurações padrão. Há um Balanceador de Carga de Aplicação que encaminha a solicitação para o respectivo grupo de destino no caminho da URL. A política de redução horizontal foi acionada devido ao baixo volume de tráfego de entrada para a aplicação.

Qual instância do EC2 será a primeira a ser encerrada pelo grupo de dimensionamento automático?

instância do EC2 foi iniciada a partir do modelo de inicialização mais antigo.

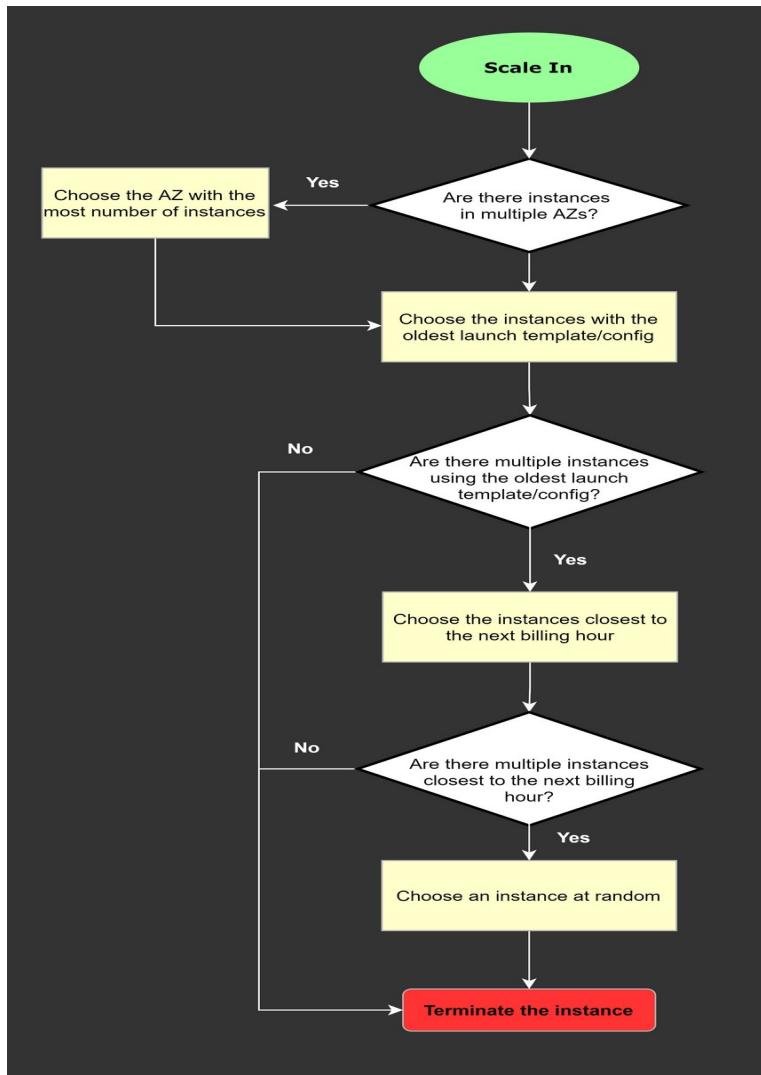
A política de encerramento padrão foi projetada para ajudar a garantir que a arquitetura da sua rede abrange as Zonas de Disponibilidade uniformemente. Com a política de encerramento padrão, o comportamento do grupo de Dimensionamento Automático é o seguinte:

1. Se houver instâncias em várias Zonas de Disponibilidade, escolha a Zona de Disponibilidade com mais instâncias e pelo menos uma instância que não esteja protegida contra redução horizontal. Se houver mais de uma Zona de Disponibilidade com esse número de instâncias, escolha a Zona de Disponibilidade com as instâncias que usam o modelo de inicialização mais antigo.
2. Determine quais instâncias desprotegidas na Zona de Disponibilidade selecionada usam o modelo de inicialização mais antigo. Se houver uma instância desse tipo, encerre-a.
3. Se houver várias instâncias a serem encerradas com base nos critérios acima, determine quais instâncias desprotegidas estão mais próximas da próxima hora de cobrança. (Isso ajuda a maximizar o

uso das suas instâncias do EC2 e a gerenciar os custos de uso do Amazon EC2.) Se houver apenas uma instância, encerre-a.

4. Se houver mais de uma instância desprotegida mais próxima da próxima hora de cobrança, escolha uma dessas instâncias aleatoriamente.

O diagrama de fluxo a seguir ilustra como a política de encerramento padrão funciona:



Portanto, a resposta correta é: **A instância do EC2 foi iniciada a partir do modelo de inicialização mais antigo.**

A opção que diz: **A instância do EC2 que tem o menor número de sessões de usuário** está incorreta porque o número de sessões de usuário normalmente não é um fator considerado pelos grupos de dimensionamento automático do Amazon EC2 ao decidir quais instâncias encerrar durante um evento de redução.

A opção que diz: **A instância do EC2 que está em execução há mais tempo** está incorreta porque a duração pela qual uma instância do EC2 está em execução não é um fator considerado principalmente pelos grupos de dimensionamento automático do Amazon EC2 ao decidir quais instâncias encerrar durante um evento de redução.

A opção que diz: **A instância será selecionada aleatoriamente pelo grupo de dimensionamento automático** está incorreta porque os grupos de dimensionamento automático do Amazon EC2 não selecionam instâncias aleatoriamente para encerramento durante um evento de redução.

Referências:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html#default-termination-policy>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>

Confira esta folha de dicas de dimensionamento automático da AWS:

<https://tutorialsdojo.com/aws-auto-scaling/>

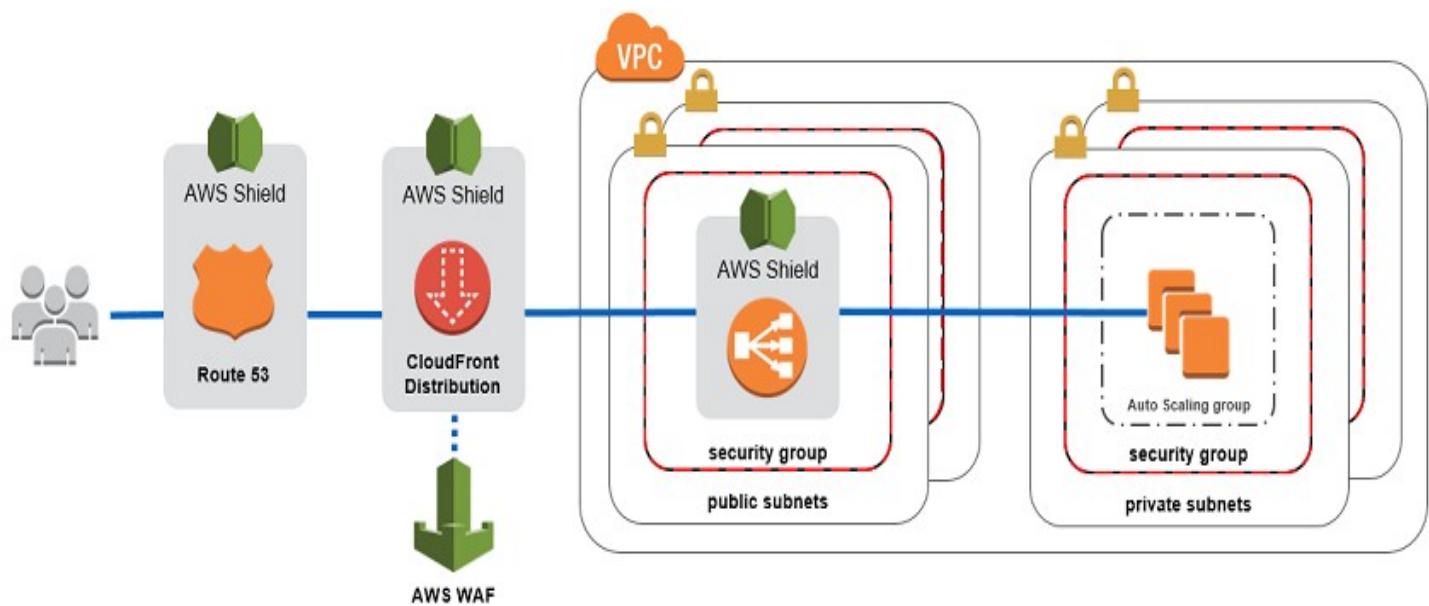
25. PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Um Arquiteto de Soluções identificou uma série de ataques DDoS ao monitorar a Amazon VPC. O Arquiteto precisa fortalecer a infraestrutura de nuvem atual para proteger os dados dos clientes. Qual das seguintes opções é a solução mais adequada para mitigar esses tipos de ataques?

Use o AWS Shield Advanced para detectar e mitigar ataques DDoS.

Para níveis mais altos de proteção contra ataques direcionados aos seus aplicativos executados em recursos do Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront e Amazon Route 53, você pode assinar o AWS Shield Advanced. Além das proteções das camadas de rede e transporte incluídas no Standard, o AWS Shield Advanced oferece detecção e mitigação adicionais contra ataques DDoS grandes e sofisticados, visibilidade quase em tempo real dos ataques e integração com o AWS WAF, um firewall de aplicações web.



O AWS Shield Advanced também oferece acesso 24x7 à Equipe de Resposta a DDoS (DRT) da AWS e proteção contra picos relacionados a DDoS em suas cobranças do Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront e Amazon Route 53.

Portanto, a resposta correta é: **Use o AWS Shield Advanced para detectar e mitigar ataques DDoS.**

A opção que diz: **Usando o AWS Firewall Manager, configure uma camada de segurança que impeça inundações de SYN, ataques de reflexão UDP e outros ataques DDoS** está incorreta porque o AWS Firewall Manager é usado principalmente para simplificar suas tarefas de administração e manutenção do AWS WAF em várias contas e recursos. Ele não protege sua VPC contra ataques DDoS.

A opção que diz: **Configurar um firewall de aplicação web usando o AWS WAF para filtrar, monitorar e bloquear tráfego HTTP** está incorreta. Embora o AWS WAF possa ajudar a bloquear padrões comuns de ataque à sua VPC, como injeção de SQL ou cross-site scripting, isso ainda não é suficiente para resistir a ataques DDoS. É melhor usar o AWS Shield neste cenário.

A opção que diz: **Uma combinação de Grupos de Segurança e Listas de Controle de Acesso à Rede para permitir apenas o acesso de tráfego autorizado à sua VPC** está incorreta. Embora o uso de uma

combinação de Grupos de Segurança e NACLs seja válido para fornecer segurança à sua VPC, isso não é suficiente para mitigar um ataque DDoS. Você deve usar o AWS Shield para melhor proteção de segurança.

Referências:

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

<https://aws.amazon.com/shield/>

Confira esta folha de dicas do AWS Shield:

<https://tutorialsdojo.com/aws-shield/>

26. PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa deseja consultar dados que residem em várias contas da AWS a partir de um data lake central. Cada conta possui seu próprio bucket do Amazon S3 que armazena dados exclusivos para sua função comercial. O acesso ao data lake deve ser concedido com base nas funções do usuário.

Qual solução minimizará a sobrecarga e os custos e, ao mesmo tempo, atenderá aos padrões de acesso necessários?

Use o AWS Lake Formation para consolidar dados de várias contas em uma única conta.

O **AWS Lake Formation** é um serviço que facilita a configuração de um data lake seguro em poucos dias. Um data lake é um repositório centralizado, com curadoria e segurança que armazena todos os seus dados, tanto em sua forma original quanto preparados para análise. Um data lake permite que você elimine silos de dados e combine diferentes tipos de análises para obter insights e orientar melhores decisões de negócios.

O Amazon S3 forma a camada de armazenamento do Lake Formation. Se você já usa o S3, normalmente começa registrando os buckets S3 existentes que contêm seus dados. O Lake Formation cria novos buckets para o data lake e importa dados para eles. A AWS sempre armazena esses dados na sua conta, e somente você tem acesso direto a eles.

The screenshot shows the AWS Lake Formation console interface. On the left, there's a navigation sidebar with sections like 'Dashboard', 'Data Catalog' (which is expanded, showing 'Catalogs', 'Databases', 'Tables' - which is selected and highlighted in yellow, 'Views', 'Data filters', 'Data sharing', 'Crawlers', 'Permissions', 'Administration', and 'Application integration settings'. The main content area is titled 'AWS Lake Formation > Tables'. It displays a table header with columns for 'Name', 'Database', 'Data ac...', 'Lake Fo...', 'Table for...', 'Compacti...', and 'Orphan fi...'. Below the table, it says 'No tables' and has a 'Create table' button. At the top right of the main area, there are buttons for 'Actions', 'Create table using a crawler', and 'Create'. A yellow arrow points from the text above to the 'Actions' button.

O AWS Lake Formation é integrado ao AWS Glue, que permite criar um catálogo de dados que descreve os conjuntos de dados disponíveis e suas respectivas aplicações comerciais. O Lake Formation permite definir políticas e controlar o acesso aos dados com conjuntos simples de "conceder e revogar permissões aos dados" em níveis granulares. Você pode atribuir permissões a usuários, funções, grupos e usuários do IAM do Active Directory usando federação. As permissões são especificadas em objetos do catálogo (como tabelas e colunas) em vez de em buckets e objetos.

Portanto, a resposta correta é: **Use o AWS Lake Formation para consolidar dados de várias contas em uma única conta.**

A opção que diz: **Usar o Amazon Data Firehose para consolidar dados de várias contas em uma única conta** está incorreta, pois configurar um Data Firehose em cada conta para mover dados para um único local é caro e impraticável. Uma abordagem melhor é configurar o compartilhamento entre contas, que é gratuito com o AWS Lake Formation.

A opção que diz: **Criar uma função AWS Lambda agendada usando o Amazon EventBridge para transferir dados de várias contas para os buckets S3 da conta central** está incorreta. Isso poderia ser feito utilizando o SDK da AWS, mas a implementação seria difícil e bastante desafiadora de gerenciar. Lembre-se de que o cenário mencionou explicitamente que a solução deve minimizar a sobrecarga de gerenciamento.

A opção que diz: **Usar o AWS Control Tower para gerenciar centralmente os buckets S3 de cada conta** está incorreta porque o serviço AWS Central Tower é usado principalmente para gerenciar e governar várias contas AWS e não apenas buckets S3. Usar o serviço AWS Lake Formation é uma escolha mais adequada.

Referências:

<https://aws.amazon.com/blogs/big-data/construindo-protetendo-e-gerenciando-lagos-de-dados-com-aws-lake-formation/>

<https://docs.aws.amazon.com/lake-formation/latest/dg/how-it-works.html>

Confira esta folha de dicas do AWS Lake Formation:

<https://tutorialsdojo.com/aws-lake-formation/>

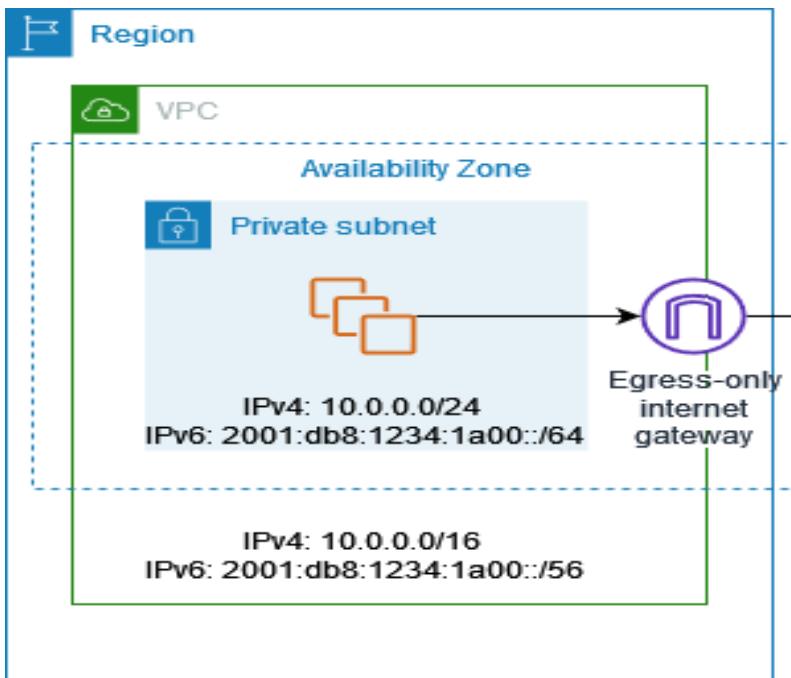
27 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa de processamento de pagamentos planeja migrar sua aplicação local para uma instância do Amazon EC2. Um bloco CIDR IPv6 está anexado à Amazon VPC da empresa. Uma política de segurança rigorosa determina que a VPC de produção deve permitir apenas a comunicação de saída via IPv6 entre a instância e a internet, mas deve impedir que a internet inicie uma conexão IPv6 de entrada. A nova arquitetura também deve permitir a inspeção e a filtragem do fluxo de tráfego. O que um arquiteto de soluções deve fazer para atender a esses requisitos?

Inicie a instância do EC2 em uma sub-rede privada e conecte um Gateway de Internet Somente de Saída à VPC para permitir a comunicação IPv6 de saída com a internet. Use o Firewall de Rede da AWS para configurar as regras necessárias para inspeção e filtragem de tráfego.

Um **gateway de internet somente de saída** é um componente de VPC escalonado horizontalmente, redundante e altamente disponível que permite a comunicação de saída via IPv6 de instâncias na sua VPC para a internet e impede que ela inicie uma conexão IPv6 com suas instâncias.



Endereços IPv6 são globalmente exclusivos e, portanto, públicos por padrão. Se você deseja que sua instância acesse a internet, mas deseja impedir que recursos na internet iniciem a comunicação com sua instância, você pode usar um gateway de internet somente de saída.

Uma **sub-rede** é um intervalo de endereços IP na sua VPC. Você pode iniciar recursos da AWS em uma sub-rede específica. Use uma **sub-rede pública** para recursos que precisam estar conectados à internet e uma **sub-rede privada** para recursos que não precisam estar conectados à internet.

O AWS Network Firewall é um serviço gerenciado que facilita a implantação de proteções de rede essenciais para todas as suas Nuvens Privadas Virtuais (VPCs) da Amazon. O serviço pode ser configurado com apenas alguns cliques e se adapta automaticamente ao seu tráfego de rede, para que você não precise se preocupar com a implantação e o gerenciamento de nenhuma infraestrutura. O AWS Network Firewall inclui recursos que oferecem proteção contra ameaças comuns à rede.

The screenshot shows the AWS Network Firewall interface. At the top, a banner reads "AWS Network Firewall Traffic Filtering". Below it, another section is titled "AWS Network Firewall Traffic Inspection".

Traffic Filtering:

- Add rule**: Info. Add the stateful rules that you need in your rule group. Each rule that you add is listed in the Rules table below.
- Protocol**: IKEV2
- Source**: Custom, IP addresses: 10.0.0.0/16, 10.0.0.0, \$VARIABLE_NAME
- Destination**: Custom, IP addresses: 10.0.0.0/16, 10.0.0.0, \$VARIABLE_NAME
- Source port**: Custom, ports: 100, 0.65535, \$VARIABLE_NAME
- Destination port**: Custom, ports: 100, 0.65535, \$VARIABLE_NAME

Traffic direction: Forward

Action: Pass

Learn more: AWS Network Firewall stateful 5 tuple rule group, Creating a stateful rule group

Rules (1)

Protocol	Source	Destination	Source port	Destination port	Direction	Action
KRB5	Any	Any	Any	Any	Forward	Pass

A message at the bottom left says: "Rule group must contain at least one rule."

Tutorials Dojo logo is visible in the bottom right corner.

O firewall com estado do AWS Network Firewall pode incorporar contexto de fluxos de tráfego, como rastreamento de conexões e identificação de protocolos, para aplicar políticas como impedir que suas VPCs acessem domínios usando um protocolo não autorizado. O sistema de prevenção de intrusão (IPS) do AWS Network Firewall fornece inspeção ativa do fluxo de tráfego para que você possa identificar e bloquear explorações de vulnerabilidades usando detecção baseada em assinatura. O AWS Network Firewall também oferece filtragem da web que pode interromper o tráfego para URLs inválidas conhecidas e monitorar nomes de domínio totalmente qualificados.

Nesse cenário, você pode usar um gateway de internet somente de saída para permitir a comunicação IPv6 de saída para a internet e, em seguida, usar o AWS Network Firewall para configurar as regras necessárias para inspeção e filtragem de tráfego.

Portanto, a resposta correta é: **inicie a instância do EC2 em uma sub-rede privada e conecte um gateway de internet somente de saída à VPC para permitir a comunicação IPv6 de saída com a internet. Use o Firewall de Rede da AWS para configurar as regras necessárias para inspeção e filtragem de tráfego.**

A opção que diz: **Inicie a instância do EC2 em uma sub-rede privada e conecte o endpoint da interface do AWS PrivateLink à VPC para controlar a comunicação IPv6 de saída com a internet. Usar o Amazon GuardDuty para configurar as regras necessárias para inspeção e filtragem de tráfego** está incorreta porque o AWS PrivateLink (também conhecido como VPC Endpoint) é apenas uma tecnologia altamente disponível e escalável que permite conectar sua VPC de forma privada aos serviços da AWS como se estivessem na sua VPC. Este serviço não é capaz de controlar a comunicação IPv6 de saída com a internet. Além disso, o serviço Amazon GuardDuty não possui os recursos necessários para realizar inspeção ou filtragem de tráfego.

A opção que diz: **Inicie a instância EC2 em uma sub-rede pública e conecte um Gateway de Internet à VPC para permitir a comunicação IPv6 de saída com a Internet. Usar o Espelhamento de Tráfego para configurar as regras necessárias para inspeção e filtragem de tráfego** está incorreta, pois um Gateway de Internet não limita nem controla nenhuma conexão IPv6 de saída. Observe que o requisito é impedir que a Internet inicie uma conexão IPv6 de entrada com sua instância. Essa solução permite que todos os tipos de tráfego iniciem uma conexão com sua instância EC2, portanto, essa opção está incorreta. Além disso, o uso do Espelhamento de Tráfego também não é apropriado. Este é apenas um recurso da Amazon VPC que você pode usar para copiar o tráfego de rede de uma interface de rede elástica do tipo interface, não para filtrar ou inspecionar o tráfego de entrada/saída.

A opção que diz: **Inicie a instância do EC2 em uma sub-rede privada e conecte um Gateway NAT à VPC para permitir a comunicação IPv6 de saída com a internet. Use o AWS Firewall Manager para configurar as regras necessárias para inspeção e filtragem de tráfego** está incorreta. Embora o Gateway NAT tenha um recurso NAT64 que converte um endereço IPv6 para IPv4, ele não impedirá que o tráfego IPv6 de entrada chegue à instância do EC2. Em vez disso, você precisa usar o Gateway de Internet somente de saída. Além disso, o AWS Firewall Manager não é capaz de realizar inspeção nem filtragem de tráfego.

Referências:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html>

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Confira esta folha de dicas do Amazon VPC:

<https://tutorialsdojo.com/amazon-vpc/>

28 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Uma organização precisa de um volume de armazenamento em bloco persistente para suportar suas cargas de trabalho de missão crítica. Os dados de backup serão armazenados em um serviço de armazenamento de objetos e, após 30 dias, transferidos para um serviço de armazenamento de arquivo para retenção de longo prazo.

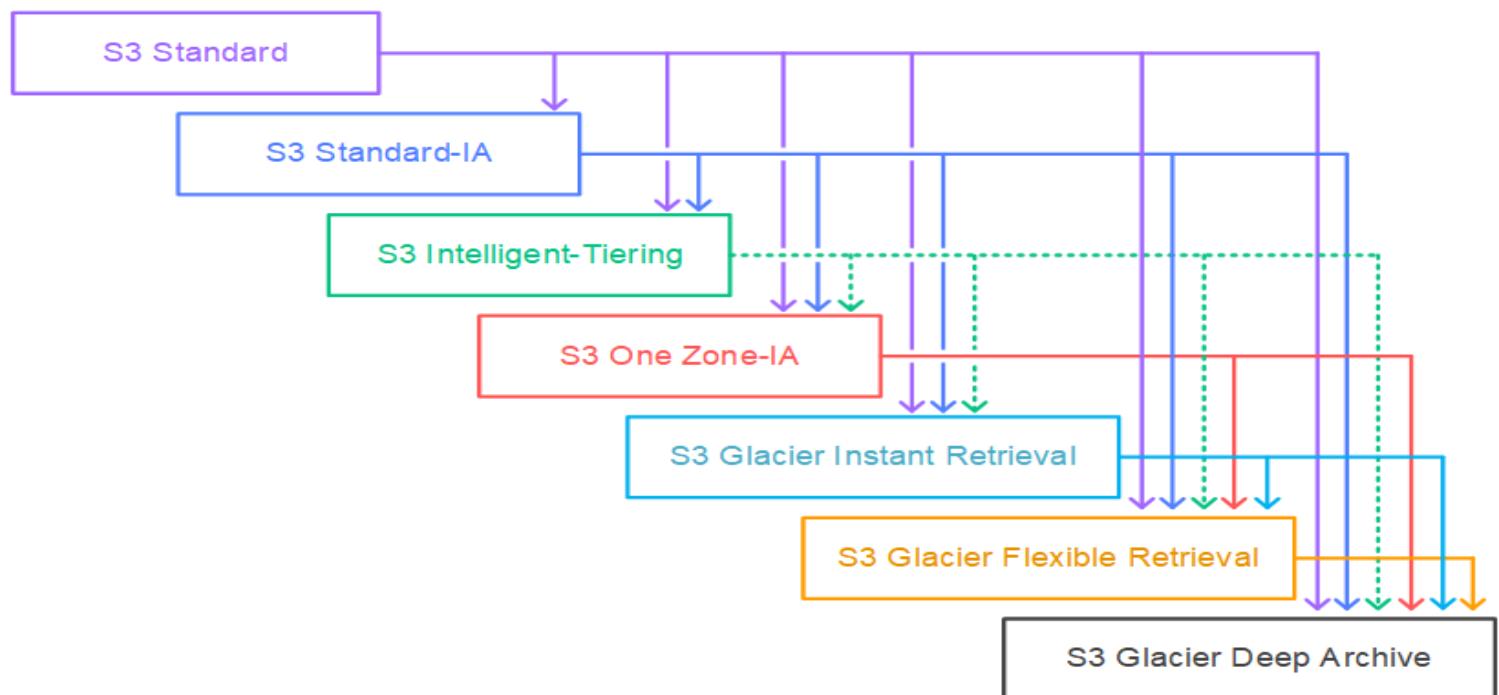
O que deve ser feito para atender ao requisito acima?

Anexe um volume do Amazon EBS à sua instância do Amazon EC2. Use o Amazon S3 para armazenar seus dados de backup e configure uma política de ciclo de vida para transferir seus objetos para o S3 Glacier Flexible Retrieval.

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 throughput e transações em qualquer escala. Uma ampla gama de cargas de trabalho, como bancos de dados relacionais e não relacionais, aplicativos corporativos, aplicativos em contêineres, mecanismos de análise de big data, sistemas de arquivos e fluxos de trabalho de mídia, são amplamente implantados no Amazon EBS.

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. Isso significa que clientes de todos os portes e setores podem usá-lo para armazenar e proteger qualquer quantidade de dados para uma variedade de casos de uso, como sites, aplicativos móveis, backup e restauração, arquivamento, aplicativos corporativos, dispositivos de IoT e análises de big data.

Em uma configuração de ciclo de vida do S3, você pode definir regras para a transição de objetos de uma classe de armazenamento para outra, economizando custos de armazenamento. O Amazon S3 oferece suporte a um modelo em cascata para a transição entre classes de armazenamento, conforme mostrado no diagrama abaixo:



Neste cenário, três serviços são necessários para implementar esta solução. As cargas de trabalho de missão crítica exigem um volume de armazenamento em bloco persistente, e o serviço projetado para isso são os volumes do Amazon EBS. A segunda carga de trabalho precisa de um serviço de armazenamento de objetos, como o Amazon S3, para armazenar seus dados de backup. O Amazon S3 permite configurar a política de ciclo de vida do S3 Standard para diferentes classes de armazenamento. Para a última, é necessário um armazenamento de arquivo, como o Amazon S3 Glacier Flexible Retrieval.

Portanto, a resposta correta é: Anexe um volume do Amazon EBS à sua instância do Amazon EC2. Use o Amazon S3 para armazenar seus dados de backup e configure uma política de ciclo de vida para transferir seus objetos para o S3 Glacier Flexible Retrieval.

A opção que diz: Anexe um volume do Amazon EBS à sua instância do Amazon EC2. Use o Amazon S3 para armazenar seus dados de backup e configure uma política de ciclo de vida para transferir seus objetos para o S3 One Zone-IA está incorreta porque essa política de ciclo de vida transferirá seus objetos para uma classe de armazenamento acessada com pouca frequência e não para uma classe de armazenamento para arquivamento de dados.

A opção que diz: Anexe um volume de armazenamento de instâncias à sua instância existente do Amazon EC2. Use o Amazon S3 para armazenar seus dados de backup e configure uma política de ciclo de vida

para transferir seus objetos para o S3 Glacier Flexible Retrieval está incorreta porque um volume de armazenamento de instâncias é simplesmente um armazenamento temporário em nível de bloco para instâncias do EC2. Além disso, você não pode anexar volumes de armazenamento de instâncias a uma instância após iniciá-la. Você pode especificar os volumes de armazenamento de instâncias para sua instância somente ao iniciá-la.

A opção que diz: **Anexar um volume de armazenamento de instância à sua instância do Amazon EC2. Usar o Amazon S3 para armazenar seus dados de backup e configurar uma política de ciclo de vida para transferir seus objetos para o S3 One Zone-IA** está incorreta. Assim como a opção anterior, o uso do volume de armazenamento de instância não é adequado para cargas de trabalho de missão crítica, pois os dados podem ser perdidos se a unidade de disco subjacente falhar, a instância parar ou se a instância for encerrada. Além disso, o Amazon S3 Glacier Flexible Retrieval é uma opção mais adequada para arquivamento de dados do que o Amazon S3 One Zone-IA.

Referências:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

<https://aws.amazon.com/s3/storage-classes/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

Tutoriais Dojo's AWS Storage Services Cheat Sheets:

<https://tutorialsdojo.com/aws-cheat-sheets-storage-services/>

29. PERGUNTA

Categoria: CSAA – Projeto de Arquiteturas Otimizadas em Custo

Uma empresa de serviços financeiros planeja migrar seu aplicativo de negociação do Microsoft Windows Server local para a Amazon Web Services (AWS). A solução deve garantir alta disponibilidade em várias Zonas de Disponibilidade e oferecer acesso de baixa latência ao armazenamento em bloco.

Qual das seguintes soluções atenderá a esses requisitos?

Configure o aplicativo de negociação em instâncias do Amazon EC2 Windows Server em duas Zonas de Disponibilidade. Use o Amazon FSx para NetApp ONTAP para criar um sistema de arquivos Multi-AZ e acessar os dados via protocolo iSCSI.

O Amazon FSx para NetApp ONTAP é um serviço AWS totalmente gerenciado que oferece armazenamento de arquivos escalável e de alto desempenho com base no sistema de arquivos ONTAP da NetApp. Ele oferece opções de armazenamento versáteis, suportando protocolos de arquivo (NFS, SMB) e bloco (iSCSI), tornando-o compatível com ambientes Windows, Linux e macOS.

Select file system type

File system options

Amazon FSx for NetApp ONTAP


 Amazon FSx for NetApp ONTAP

Amazon FSx for OpenZFS


 Amazon FSx for OpenZFS

Amazon FSx for Windows File Server


 Amazon FSx for Windows File Server

Amazon FSx for Lustre


 Amazon FSx for Lustre

Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP provides feature-rich, high-performance, and highly-reliable storage built on NetApp's popular ONTAP file system and fully managed by AWS.

- Broadly accessible from Linux, Windows, and macOS compute instances and containers (running on AWS or on-premises) via industry-standard NFS, SMB, and iSCSI protocols.
- Provides ONTAP's popular data management capabilities like Snapshots, SnapMirror (for data replication), FlexClone (for data cloning), and data compression / deduplication.
- Delivers hundreds of thousands of IOPS with consistent sub-millisecond latencies, and up to 72 GB/s of throughput.
- Offers highly-available and highly-durable single-AZ and multi-AZ deployment options, SSD storage with support for cross-region replication, and built-in, fully managed backups.
- Supports dynamic scaling of your file system to fit your storage capacity and throughput needs.
- Automatically tiers infrequently-accessed data to capacity pool storage, a fully elastic storage tier that can scale to petabytes in size and is cost-optimized for infrequently-accessed data.
- Integrates with Microsoft Active Directory (AD) to support Windows-based environments and enterprises.

O Amazon FSx para NetApp ONTAP conta com sistemas de arquivos Multi-AZ projetados para garantir disponibilidade contínua em todas as Zonas de Disponibilidade da AWS, proporcionando alta disponibilidade para suas cargas de trabalho do Windows Server. Ele oferece latências consistentes de operação de arquivos abaixo de milissegundos com armazenamento SSD, essencial para cargas de trabalho de armazenamento em bloco em ambientes Windows. O FSx para NetApp ONTAP oferece suporte total a protocolos de armazenamento em bloco como iSCSI, comumente usados em configurações do Windows Server, e funciona perfeitamente com o protocolo SMB, garantindo compatibilidade com o Windows Server e aplicativos relacionados.

Além disso, o FSx para NetApp ONTAP simplifica a migração de sistemas NetApp locais para a AWS para usuários que atualmente utilizam o armazenamento NetApp. Ele pode ser dimensionado para acomodar conjuntos de dados em escala de petabytes, tornando-o adequado para grandes ambientes Windows Server.

Portanto, a resposta correta é: **Configurar o aplicativo de negociação em instâncias do Amazon EC2 Windows Server em duas Zonas de Disponibilidade. Usar o Amazon FSx para NetApp ONTAP para criar um sistema de arquivos Multi-AZ e acessar os dados via protocolo iSCSI.**

A opção que diz: **Implantar o aplicativo de negociação em instâncias do Amazon EC2 Windows Server em duas Zonas de Disponibilidade. Usar o Amazon FSx para Windows File Server para fornecer armazenamento compartilhado entre as instâncias. Configurar o Amazon EFS com replicação entre regiões para sincronizar dados entre Zonas de Disponibilidade** está incorreta. O Amazon FSx para Windows File Server fornece apenas **armazenamento de arquivos compartilhado de baixa latência** para ambientes Windows. Ele não oferece suporte para acesso de baixa latência ao **armazenamento em bloco compartilhado**.

A opção que diz: **Implantar o aplicativo de negociação em instâncias do Amazon EC2 Windows Server em duas Zonas de Disponibilidade. Usar o Amazon Elastic File System (Amazon EFS) para fornecer armazenamento compartilhado entre as instâncias. Configurar o Amazon EFS com replicação entre regiões para sincronizar dados entre Zonas de Disponibilidade** está incorreta. Embora essa opção ofereça alta disponibilidade entre AZs, o Amazon EFS não é otimizado para cargas de trabalho do Windows e não oferece armazenamento em bloco de baixa latência.

A opção que diz: **Configurar o aplicativo de negociação em instâncias do Amazon EC2 Windows em duas Zonas de Disponibilidade. Usar o Amazon Simple Storage Service (Amazon S3) para armazenamento e configurar a replicação entre regiões para sincronizar dados entre buckets do S3 em cada Zona de Disponibilidade** está incorreta. Embora essa opção ofereça alta disponibilidade em todas as Zonas de Disponibilidade, o Amazon S3 é principalmente um armazenamento de objetos, não de blocos. Ele não oferece o acesso de baixa latência necessário para um aplicativo de negociação.

Referências:

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/high-availability-AZ.html>

Confira esta folha de dicas do Amazon FSx:

<https://tutorialsdojo.com/amazon-fsx/>

30. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Uma empresa migrou recentemente sua aplicação baseada em microsserviços para o Amazon Elastic Kubernetes Service (Amazon EKS). Como parte da migração, a empresa precisa garantir que todos os dados de configuração e credenciais confidenciais, como senhas de banco de dados e chaves de API, sejam armazenados com segurança e criptografados no repositório de chave-valor etcd do cluster Amazon EKS. Qual é a solução mais adequada para atender às necessidades da empresa?

Habilite a criptografia secreta com uma nova chave AWS KMS em um cluster Amazon EKS existente para criptografar dados confidenciais armazenados no repositório de chave-valor etcd do cluster EKS.

Habilitar a criptografia de segredos com uma nova chave do AWS Key Management Service (KMS) em um cluster existente do Amazon Elastic Kubernetes Service (EKS) é fundamental para proteger dados confidenciais armazenados no repositório de chave-valor etcd do cluster. O Amazon EKS é um serviço para executar e gerenciar aplicativos em contêineres, armazenar dados de configuração e segredos, etc., e é um repositório de dados distribuído. Por padrão, esses segredos não são criptografados, o que representa potenciais riscos à segurança. A integração do AWS KMS com o Amazon EKS permite a criptografia desses segredos, aproveitando os recursos do AWS KMS para gerenciar chaves criptográficas e controlar seu uso em serviços e aplicativos da AWS.

The screenshot shows the AWS EKS 'Create EKS cluster' wizard. On the left, a sidebar lists steps from 1 to 6: Step 1 (Configure cluster), Step 2 (Specify networking), Step 3 (Configure logging), Step 4 (Select add-ons), Step 5 (Configure selected add-ons settings), and Step 6 (Review and create). The main area is titled 'Configure cluster' and contains two sections: 'Cluster configuration' and 'Secrets encryption'. In 'Cluster configuration', the 'Name' field is set to 'test', 'Kubernetes version' is set to '1.27', and the 'Cluster service role' dropdown is set to 'eksClusterRole'. In 'Secrets encryption', the 'Turn on envelope encryption of Kubernetes secrets using KMS' checkbox is checked. The 'Tutorialspoint' logo is visible in the bottom right corner.

O processo envolve a criação de uma chave AWS KMS específica para o cluster EKS e a configuração do cluster para criptografar segredos antes de salvá-los no etcd. Essa configuração garante que todas as informações confidenciais no banco de dados etcd sejam criptografadas em repouso, aumentando a segurança dos dados. Ao adotar essa abordagem, as organizações podem aprimorar significativamente sua postura de segurança, garantindo que dados e credenciais confidenciais sejam protegidos de acordo com

os padrões do setor e os requisitos de conformidade, mantendo assim a confidencialidade e a integridade dos dados em seus ambientes Kubernetes.

Portanto, a resposta correta é: **Habilite a criptografia secreta com uma nova chave AWS KMS em um cluster Amazon EKS existente para criptografar dados confidenciais armazenados no repositório de chave-valor etcd do cluster EKS.**

A opção que diz: **Usar o AWS Secrets Manager com uma nova chave AWS KMS para gerenciar e armazenar com segurança dados confidenciais no repositório de chave-valor etcd do cluster EKS** está incorreta. O AWS Secrets Manager é uma ferramenta poderosa para gerenciar segredos, mas não aborda diretamente a criptografia de dados no repositório de chave-valor etcd de um cluster EKS. O Secrets Manager se concentra mais no gerenciamento e na recuperação de segredos do que na criptografia de dados no etcd.

A opção que diz: **Habilitar a criptografia de volume padrão do Amazon EBS para a conta com uma nova chave AWS KMS para garantir a criptografia de dados confidenciais no cluster Amazon EKS** está incorreta. Habilitar a criptografia de volume padrão do Amazon EBS é uma maneira de garantir que os dados em repouso nos volumes EBS sejam criptografados. No entanto, os volumes EBS são usados principalmente para armazenamento persistente dos nós de trabalho. Eles não estão diretamente relacionados ao armazenamento de dados de configuração e credenciais confidenciais no repositório de chave-valor etcd do cluster EKS.

A opção que diz: **Usar as opções padrão do Amazon EKS e o driver da Interface de Armazenamento de Contêineres (CSI) do Amazon Elastic Block Store (Amazon EBS) como um complemento para armazenar dados confidenciais com segurança no cluster do Amazon EKS** está incorreta. O driver CSI do Amazon EBS habilita volumes do Amazon Elastic Block Store (EBS) como armazenamento persistente para aplicativos Kubernetes em execução no Amazon EKS. Embora isso possa fornecer armazenamento persistente seguro para seus microsserviços, não atende ao requisito específico de armazenar com segurança dados confidenciais no repositório de chave-valor etcd do cluster EKS.

Referências:

<https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html>
<https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/>
<https://docs.aws.amazon.com/eks/latest/userguide/enable-kms.html>

Confira esta folha de dicas do serviço Amazon Elastic Kubernetes:

<https://tutorialsdojo.com/amazon-elastic-kubernetes-service-eks/>

31. PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa global de TI com escritórios em todo o mundo possui várias contas na AWS. Para aumentar a eficiência e reduzir custos, o Diretor de Informações (CIO) deseja configurar uma solução que gerencie centralmente seus recursos na AWS. Isso permitirá que eles adquiram recursos da AWS centralmente e compartilhem recursos como AWS Transit Gateways, configurações do AWS License Manager ou regras do Amazon Route 53 Resolver entre suas diversas contas.

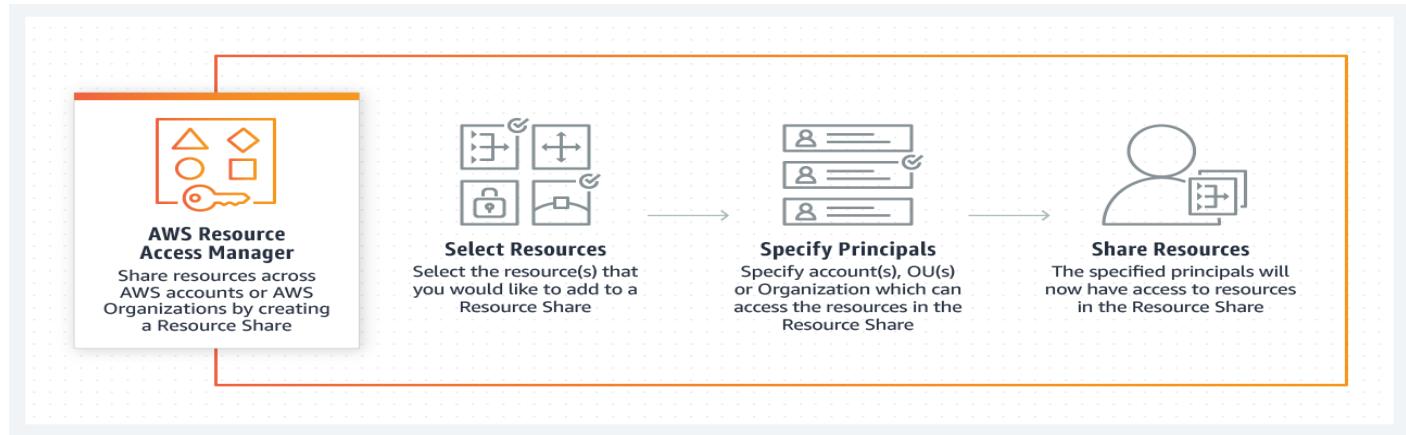
Como arquiteto de soluções, qual combinação de opções você deve implementar neste cenário? (Selecione DUAS.)

Consolide todas as contas da empresa usando o AWS Organizations.

Use o serviço AWS Resource Access Manager (RAM) para compartilhar seus recursos com suas contas da AWS de forma fácil e segura.

O AWS Resource Access Manager (RAM) é um serviço que permite compartilhar recursos da AWS de forma fácil e segura com qualquer conta da AWS ou dentro da sua organização. 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.

Muitas organizações usam múltiplas contas para criar isolamento administrativo ou de faturamento e limitar o impacto de erros. O RAM elimina a necessidade de criar recursos duplicados em múltiplas contas, reduzindo a sobrecarga operacional de gerenciar esses recursos em cada conta que você possui. Você pode criar recursos centralmente em um ambiente multicontas e usar o RAM para compartilhá-los entre contas em três etapas simples: criar um Compartilhamento de Recursos, especificar recursos e especificar contas. O RAM está disponível para você sem custo adicional.



Você pode adquirir recursos da AWS centralmente e usar o RAM para compartilhar recursos, como sub-redes ou configurações do Gerenciador de Licenças, com outras contas. Isso elimina a necessidade de provisionar recursos duplicados em todas as contas em um ambiente com várias contas, reduzindo a sobrecarga operacional de gerenciar esses recursos em cada conta.

O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas da AWS em uma organização que você cria e gerencia centralmente. Com o Organizations, você pode criar contas de membros e convidar contas existentes para ingressar na sua organização. Você pode organizar essas contas em grupos e anexar controles baseados em políticas.

Portanto, a combinação correta de opções neste cenário é:

- **Consolide todas as contas da empresa usando o AWS Organizations.**
- **Use o serviço AWS Resource Access Manager (RAM) para compartilhar seus recursos com suas contas da AWS de forma fácil e segura.**

A opção que diz: **Use o serviço AWS Identity and Access Management para configurar o acesso entre contas que compartilhará seus recursos com suas contas da AWS de forma fácil e segura** está incorreta. Embora seja possível delegar acesso a recursos que estão em diferentes contas da AWS usando o IAM, esse processo é extremamente tedioso e acarreta muita sobrecarga operacional, pois você precisa configurar manualmente o acesso entre contas para cada conta da AWS da empresa. Uma solução melhor é usar o AWS Resources Access Manager.

A opção que diz: **Use a AWS Control Tower para compartilhar seus recursos com suas contas da AWS de forma fácil e segura** está incorreta, pois a AWS Control Tower simplesmente oferece a maneira mais fácil de configurar e governar um ambiente AWS novo, seguro e com várias contas. Este não é o serviço mais adequado para compartilhar seus recursos com segurança entre contas da AWS ou dentro da sua organização. Em vez disso, você precisa usar o AWS Resources Access Manager (RAM).

A opção que diz: **Consolidar todas as contas da empresa usando o AWS ParallelCluster** está incorreta, pois o AWS ParallelCluster é simplesmente uma ferramenta de gerenciamento de cluster de código aberto com suporte da AWS que facilita a implantação e o gerenciamento de clusters de Computação de Alto Desempenho (HPC) na AWS. Nesse cenário específico, é mais apropriado usar o AWS Organizations para consolidar todas as suas contas da AWS.

Referências:

<https://aws.amazon.com/ram/>

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

Categoria: CSAA - Design de Arquiteturas de Alto Desempenho

Um popular site de mídia social utiliza uma distribuição web do Amazon CloudFront para fornecer conteúdo estático a milhões de usuários em todo o mundo. Recentemente, o site recebeu diversas reclamações sobre longos tempos de login. Além disso, há casos em que usuários encontram erros HTTP 504. O gerente instruiu a equipe a reduzir significativamente o tempo de login e otimizar ainda mais o sistema.

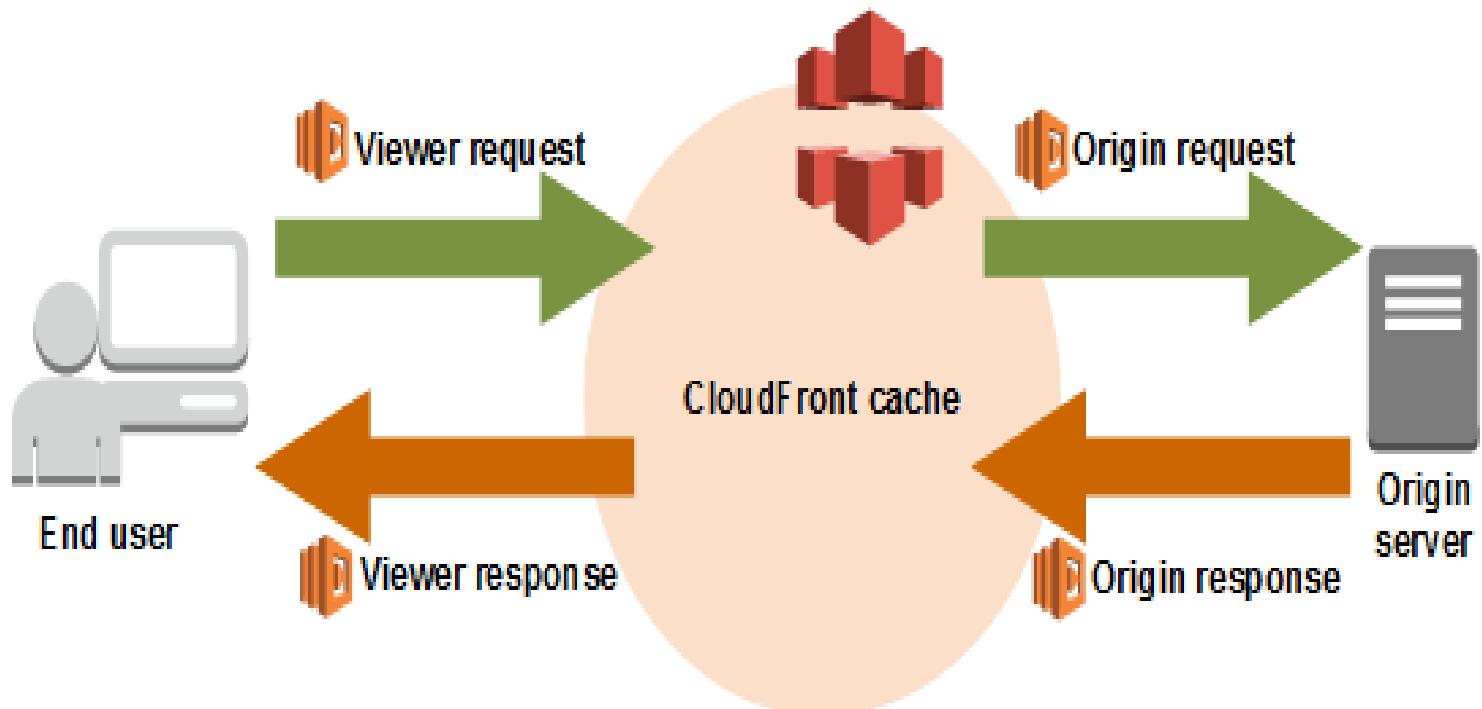
Qual das seguintes opções deve ser usada em conjunto para configurar uma solução econômica que melhore o desempenho do aplicativo? (Selecione DUAS.)

Implemente um failover de origem criando um grupo de origem que inclua duas origens. Atribua uma como origem primária e a outra como secundária, o que permite que o CloudFront alterne automaticamente para a origem primária caso encontre respostas de falha de código de status HTTP específicas.

Personalize o conteúdo que a distribuição web do CloudFront entrega aos seus usuários usando o Lambda@Edge, o que permite que suas funções do AWS Lambda executem o processo de autenticação em locais da AWS mais próximos dos usuários.

O Lambda @Edge permite executar funções do Lambda para personalizar o conteúdo entregue pelo CloudFront, executando-as em locais da AWS mais próximos do visualizador. As funções são executadas em resposta a eventos do CloudFront, sem provisionar ou gerenciar servidores. Você pode usar funções do Lambda para alterar solicitações e respostas do CloudFront nos seguintes pontos:

- Após o CloudFront receber uma solicitação de um visualizador (solicitação do visualizador)
- Antes do CloudFront encaminhar a solicitação para a origem (origin request)
- Após o CloudFront receber a resposta da origem (resposta de origem)
- Antes que o CloudFront encaminhe a resposta ao visualizador (resposta do visualizador)



No cenário em questão, você pode usar o Lambda @Edge para permitir que suas funções do Lambda personalizem o conteúdo entregue pelo CloudFront e executem o processo de autenticação em locais da AWS mais próximos dos usuários. Além disso, você pode configurar um failover de origem criando um grupo de origem com duas origens, uma como origem primária e a outra como segunda origem, para a qual o CloudFront alterna automaticamente quando a origem primária falha. Isso aliviaria os erros HTTP 504 ocasionais que os usuários estão enfrentando.

Portanto, as respostas corretas são:

- Personalize o conteúdo que a distribuição web do CloudFront entrega aos seus usuários usando o Lambda @Edge , o que permite que suas funções do AWS Lambda executem o processo de autenticação em locais da AWS mais próximos dos usuários.
- Implemente um failover de origem criando um grupo de origem que inclua duas origens. Atribua uma como origem primária e a outra como secundária, o que permite que o CloudFront alterne automaticamente para a origem primária caso encontre respostas de falha de código de status HTTP específicas.

A opção que diz: **Estabeleça várias VPCs da Amazon em diferentes regiões da AWS e configure uma VPC de trânsito para interconectar todos os seus recursos. Para processar as solicitações mais rapidamente, configurar funções do AWS Lambda em cada região com o serviço AWS Serverless Application Model (SAM)** está incorreta pelo mesmo motivo mencionado acima. Embora configurar várias VPCs em diferentes regiões conectadas apenas a uma VPC de trânsito seja válido, essa solução ainda acarreta custos mais altos de configuração e manutenção. Uma opção mais econômica seria usar o Lambda @Edge .

A opção que diz: **Configure sua origem para adicionar uma Cache-Control max-aged diretiva aos seus objetos e especifique o maior valor prático para max-age aumentar a taxa de acerto do cache da sua distribuição do CloudFront** está incorreta, pois melhorar a taxa de acerto do cache para a distribuição do CloudFront é irrelevante neste cenário. Você só pode melhorar o desempenho do cache aumentando a proporção de solicitações do visualizador que são atendidas pelos caches de borda do CloudFront em vez de irem para os servidores de origem em busca de conteúdo. No entanto, observe que o problema nesse cenário é o processo lento de autenticação dos seus usuários globais e não apenas o armazenamento em cache dos objetos estáticos.

A opção que diz: **Implante seu aplicativo em várias regiões da AWS para acomodar seus usuários ao redor do mundo. Configurar um registro do Route 53 com política de roteamento de latência para rotear o tráfego de entrada para a região que oferece a melhor latência para o usuário** está incorreta. Embora isso possa resolver o problema de desempenho, essa solução acarreta um custo de implementação significativo, pois você precisa implantar seu aplicativo em várias regiões da AWS. Lembre-se de que o cenário solicita uma solução que melhore o desempenho do aplicativo com custo mínimo .

Referências:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html>

Confira estas folhas de dicas do Amazon CloudFront e do AWS Lambda:

<https://tutorialsdojo.com/amazon-cloudfront/>

<https://tutorialsdojo.com/aws-lambda/>

33 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa migrou recentemente seus aplicativos para a AWS. A equipe de auditoria precisa ser capaz de avaliar se os serviços que a empresa utiliza atendem aos padrões comuns de segurança e regulamentação. Um arquiteto de soluções precisa fornecer à equipe um relatório com todos os documentos relacionados à conformidade de sua conta.

Qual ação um arquiteto de soluções deve considerar?

Use o AWS Artifact para visualizar os relatórios de segurança, bem como outras informações relacionadas à conformidade da AWS.

O AWS Artifact é o seu recurso central para obter informações relevantes sobre conformidade. Ele oferece acesso sob demanda aos relatórios de segurança e conformidade da AWS e a contratos online selecionados. Os relatórios disponíveis no AWS Artifact incluem nossos relatórios de Controle de Organização de Serviços (SOC), relatórios do Setor de Cartões de Pagamento (PCI) e certificações de órgãos de acreditação em diversas regiões e setores de conformidade que validam a implementação e a

eficácia operacional dos controles de segurança da AWS. Os contratos disponíveis no AWS Artifact incluem o Adendo de Associado Comercial (BAA) e o Acordo de Confidencialidade (NDA).

The screenshot shows the AWS Artifact interface. On the left, there's a sidebar with 'Reports' selected, showing 'Agreements'. The main content area displays three artifacts:

- APRA CPG 234 Workbook**:
Reporting period: Valid beginning 07/01/2019
Description: The AWS Workbook for Australian Prudential Regulation Authority (APRA)'s CPG 234 "Information Security" (AWS APRA CPG 234 Workbook) is intended as a reference and supporting document to assist financial services institutions (FIs) regulated by APRA in their own preparation for a compliance review with APRA. Where applicable, under the AWS shared responsibility model, the workbook provides supporting details and references in relation to AWS to assist FIs when adapting APRA CPG 234 for their workloads on AWS.
Get this artifact
- ASIP HDS Certification**:
Reporting period: Valid from 01/14/2019 to 01/13/2022
Description: This certification, issued by an independent third-party auditor, validates that AWS complies with the ASIP HDS standard. The ASIP HDS standard provides technical and governance measures to secure and protect personal health data.
Get this artifact
- AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline on Use of Cloud Computing Services**:
Reporting period: Valid beginning 04/16/2019
Description: The AWS Workbook for Korean Financial Security Institute (FSI)'s Guideline "Guideline on Use of Cloud Computing Services in Financial Industry" is intended as a reference and supporting document to assist customers in their own preparation for a compliance review.
Get this artifact

Todas as contas da AWS têm acesso ao AWS Artifact. Usuários root e usuários do IAM com permissões de administrador podem baixar todos os artefatos de auditoria disponíveis para suas contas, concordando com os termos e condições associados. Você precisará conceder aos usuários do IAM com permissões não administrativas acesso ao AWS Artifact usando as permissões do IAM. Isso permite que você conceda a um usuário acesso ao AWS Artifact enquanto restringe o acesso a outros serviços e recursos em sua conta da AWS.

Portanto, a resposta correta neste cenário é: **Use o AWS Artifact para visualizar os relatórios de segurança, bem como outras informações relacionadas à conformidade da AWS.**

A opção que diz: **Executar uma tarefa de avaliação do Amazon Inspector para baixar todas as informações relacionadas à conformidade da AWS** está incorreta. O Amazon Inspector é simplesmente uma ferramenta de segurança para detectar vulnerabilidades em cargas de trabalho da AWS. Para este cenário, é melhor usar os relatórios de segurança prontamente disponíveis no AWS Artifact.

A opção que diz: **Executar uma tarefa do Amazon Macie para visualizar o Controle de Organização de Serviços (SOC), o Setor de Cartões de Pagamento (PCI) e outros relatórios de conformidade do AWS Certificate Manager (ACM)** está incorreta porque o ACM é apenas um serviço que permite provisionar, gerenciar e implantar facilmente certificados SSL/TLS (Secure Sockets Layer/Transport Layer Security) públicos e privados para uso com serviços da AWS e seus recursos internos conectados. Este serviço não armazena certificações ou documentos relacionados à conformidade.

A opção que diz: **Exibir todos os relatórios de conformidade de segurança da AWS no AWS Security Hub** está incorreta porque o AWS Security Hub fornece apenas uma visão abrangente dos seus alertas de segurança de alta prioridade e da postura de segurança em suas contas da AWS.

Referências:

<https://aws.amazon.com/artifact/getting-started/>

<https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html>

Confira esta folha de dicas do AWS Artifact:

<https://tutorialsdojo.com/aws-artifact/>

34 . PERGUNTA

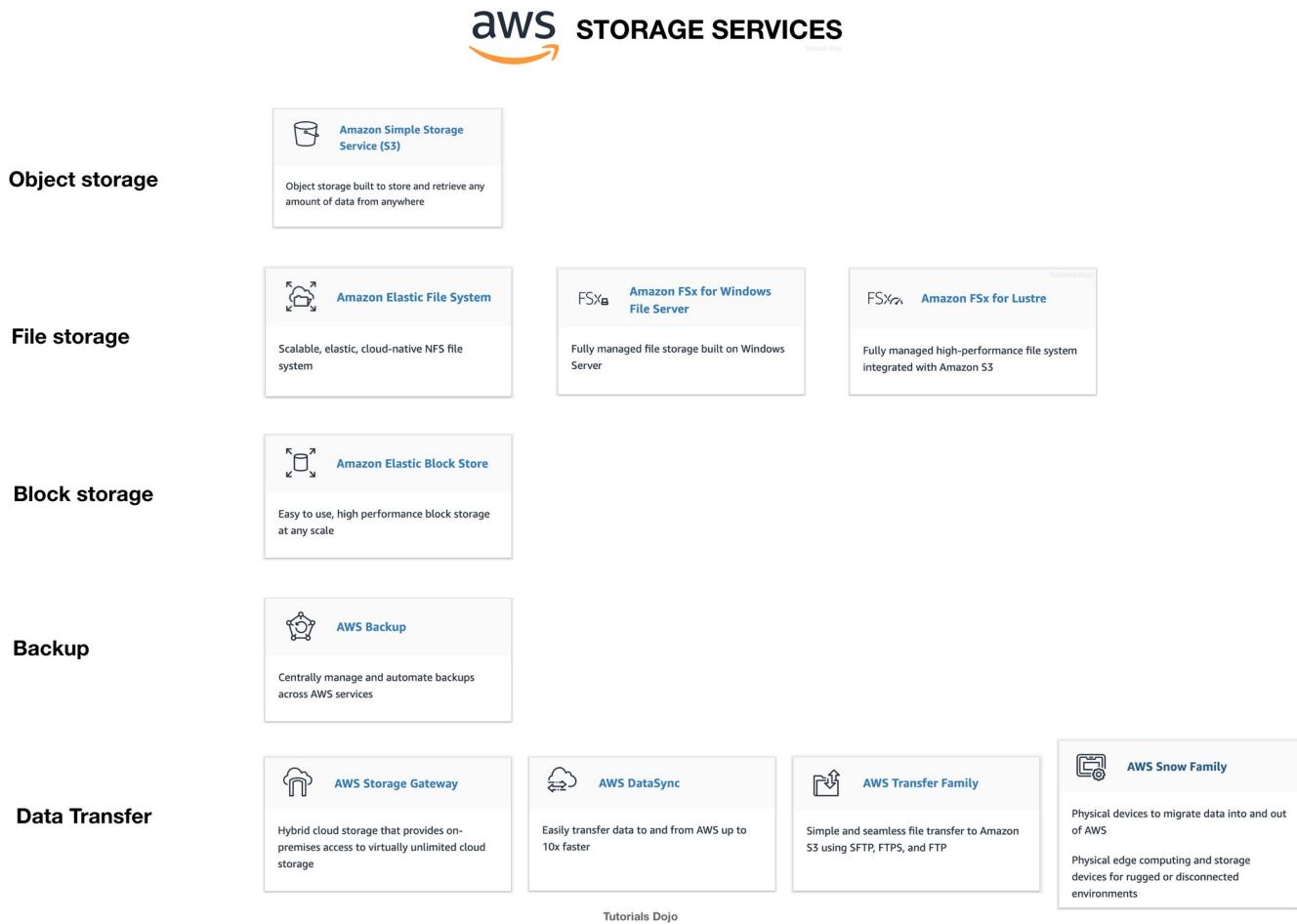
Categoria: CSAA - Design de Arquiteturas de Alto Desempenho

Um aplicativo de negociação Forex com tecnologia de IA consome milhares de conjuntos de dados para treinar seu modelo de aprendizado de máquina. A carga de trabalho do aplicativo requer um armazenamento paralelo de alto desempenho para processar os conjuntos de dados de treinamento simultaneamente. Ele também precisa de um armazenamento frio com boa relação custo-benefício para arquivar os conjuntos de dados que geram baixo lucro.

Qual dos seguintes serviços de armazenamento da Amazon o desenvolvedor deve usar?

Use o Amazon FSx For Lustre e o Amazon S3 para armazenamento quente e frio, respectivamente.

Armazenamento quente refere-se ao armazenamento que armazena dados acessados com frequência (dados quentes). **Armazenamento morno** refere-se ao armazenamento que armazena dados acessados com menos frequência (dados mornos). **Armazenamento frio** refere-se ao armazenamento que armazena dados raramente acessados (dados frios). Em termos de preço, quanto mais frios os dados, mais barato é armazená-los e mais custoso é acessá-los quando necessário.



O **Amazon FSx para Lustre** é um sistema de arquivos de alto desempenho para processamento rápido de cargas de trabalho. O Lustre é um popular **sistema de arquivos paralelos de código aberto** que armazena dados em vários servidores de arquivos de rede para maximizar o desempenho e reduzir gargalos.

O **Amazon FSx for Windows File Server** é um sistema de arquivos Microsoft Windows totalmente gerenciado com suporte total ao protocolo SMB, Windows NTFS e integração com o Microsoft Active Directory (AD).

O **Amazon Elastic File System** é um serviço de armazenamento de arquivos totalmente gerenciado que facilita a configuração e o dimensionamento do armazenamento de arquivos na Amazon Cloud.

O **Amazon S3** é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e desempenho líderes do setor. O S3 oferece diferentes níveis de armazenamento para

diferentes casos de uso (dados acessados com frequência, dados acessados com pouca frequência e dados raramente acessados).

A questão tem dois requisitos:

- Armazenamento ativo paralelo de alto desempenho para processar os conjuntos de dados de treinamento simultaneamente.
- Armazenamento a frio econômico para manter os conjuntos de dados arquivados que são acessados com pouca frequência

Neste caso, podemos usar o **Amazon FSx para Lustre** para o primeiro requisito, pois ele fornece um sistema de arquivos paralelo de alto desempenho para dados ativos. Para o segundo requisito, podemos usar o Amazon S3 para armazenar dados inativos. O Amazon S3 oferece suporte a um sistema de armazenamento inativo por meio do Amazon S3 Glacier / Glacier Deep Archive.

Portanto, a resposta correta é: **use o Amazon FSx For Lustre e o Amazon S3 para armazenamento quente e frio, respectivamente.**

A opção que diz: **Usar volumes Amazon FSx para Lustre e Amazon EBS Provisioned IOPS SSD (io1) para armazenamento quente e frio, respectivamente,** está incorreta, pois os volumes Provisioned IOPS SSD (io1) são projetados principalmente para armazenar dados quentes (dados acessados com frequência) usados em cargas de trabalho com uso intensivo de E/S. O EBS oferece uma opção de armazenamento chamada "Cold HDD", mas, devido ao seu preço, não é ideal para arquivamento de dados. O EBS Cold HDD é muito mais caro que o Amazon S3 Glacier/Glacier Deep Archive e é frequentemente utilizado em aplicativos onde dados frios sequenciais são lidos com menos frequência.

A opção que diz: **Usar o Amazon Elastic File System e o Amazon S3 para armazenamento quente e frio, respectivamente,** está incorreta. Embora o EFS suporte acesso simultâneo aos dados, ele não possui a capacidade de alto desempenho normalmente necessária para cargas de trabalho de aprendizado de máquina.

A opção que diz: **Usar o Amazon FSx para Windows File Server e o Amazon S3 para armazenamento quente e frio, respectivamente,** está incorreta porque o Amazon FSx para Windows File Server não tem um sistema de arquivos paralelo, ao contrário do Lustre.

Referências:

<https://aws.amazon.com/fsx/>

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-storage-optimization/aws-storage-services.html>

<https://aws.amazon.com/blogs/startups/escolhendo-o-armazenamento-de-dados-certo-para-sua-carga-de-trabalho/>

Confira esta folha de dicas do Amazon FSx:

<https://tutorialsdojo.com/amazon-fsx/>

35 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa usa o Amazon S3 para armazenar dados acessados com frequência. Quando um objeto é criado ou excluído, o bucket do S3 envia uma notificação de evento para a fila do Amazon SQS. Um arquiteto de soluções precisa criar uma solução que notifique a equipe de desenvolvimento e operações sobre os objetos criados ou excluídos.

Qual das seguintes opções atenderia a esse requisito?

Crie um tópico do Amazon SNS e configure duas filas SQS para assinar o tópico. Conceda permissão ao S3 para enviar notificações ao SNS e atualize o bucket para usar o novo tópico do SNS.

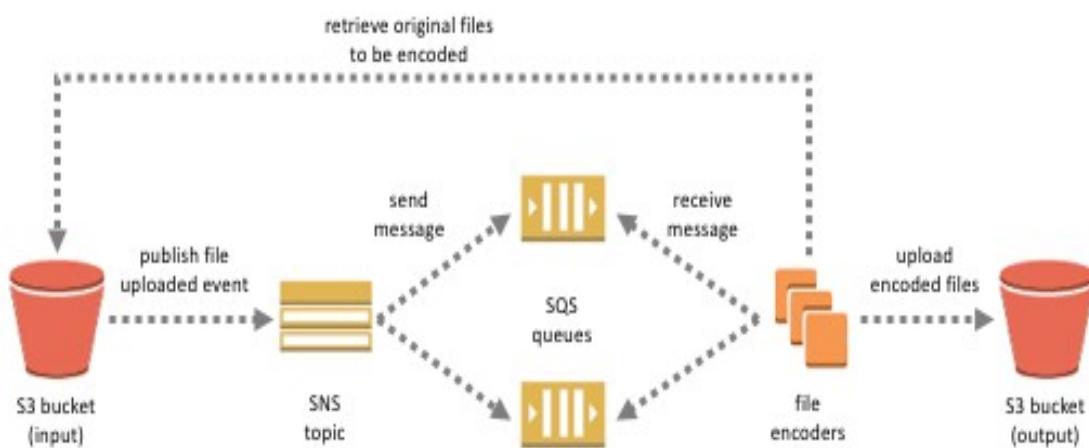
O recurso de notificação do **Amazon S3** permite que você receba notificações quando determinados eventos ocorrerem no seu bucket. Para habilitar notificações, você precisa primeiro adicionar uma configuração

de notificação que identifique os eventos que você deseja que o Amazon S3 publique e os destinos para onde você deseja que o Amazon S3 envie as notificações. Você armazena essa configuração no sub-recurso de notificação associado a um bucket.

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

- Tópico do Amazon Simple Notification Service (Amazon SNS)
- Fila do Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda

No Amazon SNS, o cenário de fanout ocorre quando uma mensagem publicada em um tópico do SNS é replicada e enviada para vários endpoints, como filas do Amazon SQS, endpoints HTTP(S) e funções Lambda. Isso permite o processamento assíncrono paralelo.



Por exemplo, você pode desenvolver um aplicativo que publique uma mensagem em um tópico do SNS sempre que um pedido de um produto for feito. Assim, as filas do SQS inscritas no tópico do SNS receberão notificações idênticas para o novo pedido. Uma instância de servidor do Amazon Elastic Compute Cloud (Amazon EC2) conectada a uma das filas do SQS pode lidar com o processamento ou o atendimento do pedido. E você pode conectar outra instância de servidor do Amazon EC2 a um data warehouse para análise de todos os pedidos recebidos.

Com base no cenário fornecido, a configuração existente envia a notificação de evento para uma fila do SQS. Como você precisa enviar a notificação para a equipe de desenvolvimento e operações, pode usar uma combinação do Amazon SNS e do SQS. Usando o padrão de distribuição de mensagens, você pode criar um tópico e usar duas filas do Amazon SQS para assinar o tópico. Se o Amazon SNS receber uma notificação de evento, ele publicará a mensagem para ambos os assinantes.

Observe que as notificações de eventos do Amazon S3 são projetadas para serem entregues pelo menos uma vez e para apenas um destino. Não é possível anexar dois ou mais tópicos do SNS ou filas do SQS para notificações de eventos do S3. Portanto, você deve enviar a notificação de eventos para o Amazon SNS.

Portanto, a resposta correta é: **criar um tópico do Amazon SNS e configurar duas filas SQS para assinar o tópico. Conceder permissão ao S3 para enviar notificações ao SNS e atualizar o bucket para usar o novo tópico do SNS.**

A opção que diz: **Configurar outra fila SQS para a outra equipe. Conceder permissão ao S3 para enviar uma notificação à segunda fila SQS** está incorreta porque você só pode adicionar 1 SQS ou SNS por vez para notificação de eventos do Amazon S3. Se precisar enviar os eventos para vários assinantes, você deve implementar um padrão de distribuição de mensagens com o Amazon SNS e o Amazon SQS.

A opção que diz: **Criar um novo tópico FIFO do Amazon SNS para a outra equipe. Conceder permissão ao S3 para enviar a notificação ao segundo tópico do SNS** está incorreta. Conforme mencionado na opção anterior, você só pode adicionar 1 SQS ou SNS por vez para notificação de eventos do Amazon S3. Além disso, nem o tópico FIFO do Amazon SNS nem a fila FIFO do Amazon SQS são necessários neste cenário.

Ambos podem ser usados em conjunto para fornecer ordenação rigorosa de mensagens e desduplicação de mensagens. Os recursos FIFO de cada um desses serviços trabalham juntos para atuar como um serviço totalmente gerenciado para integrar aplicativos distribuídos que exigem consistência de dados quase em tempo real.

A opção que diz: **Configurar um tópico do Amazon SNS e configurar duas filas do SQS para consultar o tópico do SNS. Conceder permissão ao S3 para enviar notificações ao SNS e atualizar o bucket para usar o novo tópico do SNS** está incorreta porque você não pode consultar o Amazon SNS. Em vez de configurar filas para consultar o Amazon SNS, você deve configurar cada fila do Amazon SQS para assinar o tópico do SNS.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html#notification-how-to-overview>

<https://docs.aws.amazon.com/sns/latest/dg/welcome.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

36. PERGUNTA

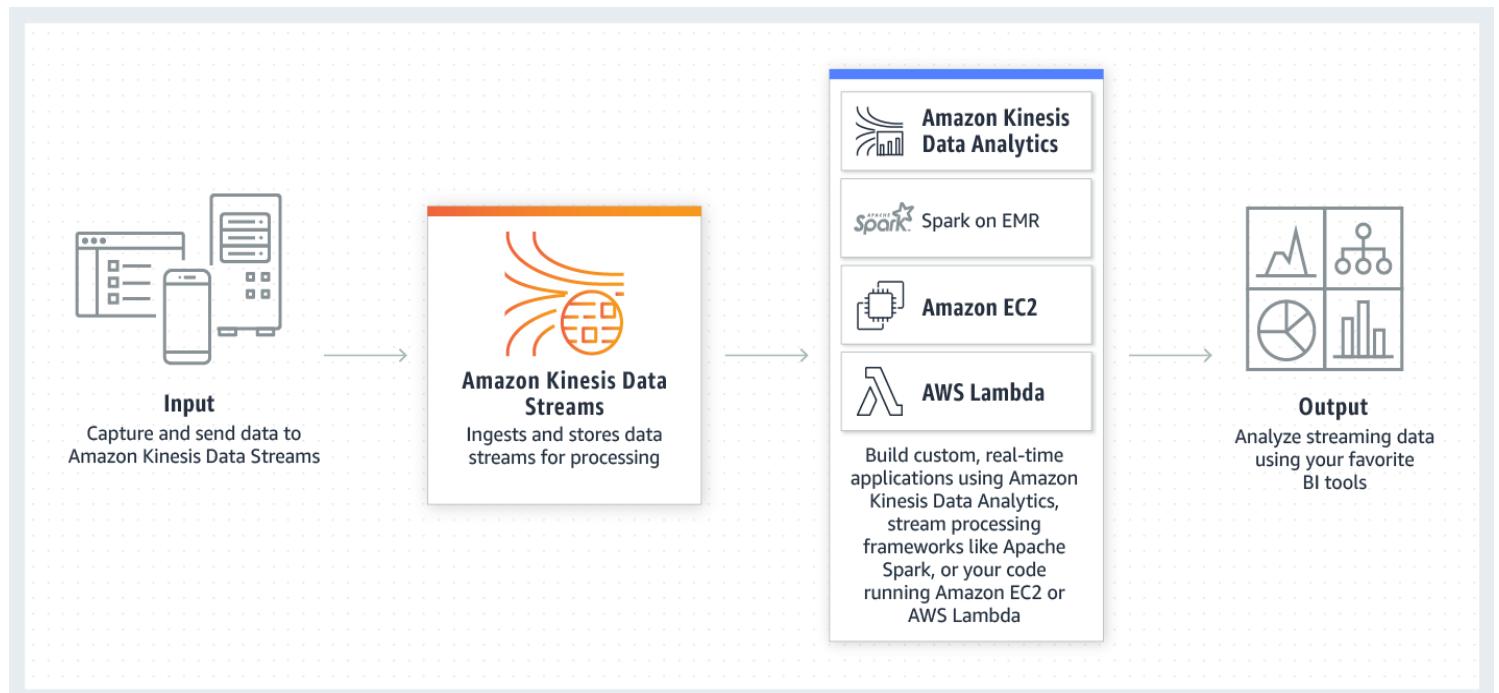
Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma organização de saúde deseja construir um sistema que possa prever o abuso de medicamentos prescritos. A organização coletará dados em tempo real de diversas fontes, incluindo Informações Pessoais Identificáveis (PII). É crucial que essas informações confidenciais sejam anonimizadas antes de serem inseridas em um banco de dados NoSQL para processamento posterior.

Qual solução atenderia aos requisitos?

Ingira dados em tempo real usando o Amazon Kinesis Data Stream. Use uma função do AWS Lambda para anonimizar as PII e armazene-as no Amazon DynamoDB.

O **Amazon Kinesis Data Streams (KDS)** é um serviço de streaming de dados em tempo real, altamente escalável e durável. O KDS pode capturar continuamente gigabytes de dados por segundo de centenas de milhares de fontes.



O Kinesis Data Streams integra-se perfeitamente ao AWS Lambda, que pode ser utilizado para transformar e anonimizar as Informações Pessoais Identificáveis (PII) em trânsito antes do armazenamento. Isso garante que informações confidenciais sejam devidamente anonimizadas o mais rápido possível, reduzindo significativamente o risco de violações de dados ou de privacidade. Por fim, os dados anonimizados são armazenados no Amazon DynamoDB, um banco de dados NoSQL adequado para lidar com os dados processados.

Portanto, a resposta correta é: **Ingerir dados em tempo real usando o Amazon Kinesis Data Stream. Usar uma função do AWS Lambda para anonimizar as PII e armazená-las no Amazon DynamoDB.**

A opção que diz: **Criar um data lake no Amazon S3 e usá-lo como armazenamento primário para dados de saúde de pacientes. Usar um gatilho do S3 para executar uma função do AWS Lambda que realiza a anonimização. Enviar os dados anonimizados para o Amazon DynamoDB** está incorreta. Essa abordagem não garante a anonimização dos dados antes de eles serem enviados ao DynamoDB. Os dados serão primeiro armazenados no S3 e depois anonimizados, potencialmente expondo informações confidenciais. Isso viola o princípio de garantir que as PII sejam anonimizadas antes do armazenamento.

A opção que diz: **Transmitir os dados em uma tabela do Amazon DynamoDB. Habilitar os fluxos do DynamoDB e configurar uma função que realiza a anonimização em itens recém-gravados** está incorreta. Os fluxos do DynamoDB normalmente operam com base em alterações em dados que já foram gravados no banco de dados. Portanto, as PII serão armazenadas no DynamoDB antes que a função de anonimização seja acionada, o que pode ser um problema de privacidade.

A opção que diz: **Implantar um fluxo do Amazon Data Firehose para capturar e transformar os dados de streaming. Entregar os dados anonimizados ao Amazon Redshift para análise** está incorreta. O requisito era armazenar os dados em um banco de dados NoSQL. O Amazon Redshift é principalmente uma solução de data warehouse construída em um modelo de banco de dados relacional, não em um modelo NoSQL, o que torna essa opção inadequada para atender aos requisitos fornecidos.

Referências:

<https://aws.amazon.com/kinesis/data-streams/>

<https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html>

Confira esta folha de dicas do Amazon Kinesis:

<https://tutorialsdojo.com/amazon-kinesis/>

37 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa de ensino online hospeda seu aplicativo Microsoft .NET e-Learning em um servidor Windows em seu data center local. O aplicativo utiliza um Oracle Database Standard Edition como banco de dados de back-end.

A empresa deseja uma solução de alto desempenho para migrar essa carga de trabalho para a nuvem AWS, aproveitando a alta disponibilidade da nuvem. O processo de migração deve minimizar as mudanças de desenvolvimento e o ambiente deve ser mais fácil de gerenciar.

Qual das seguintes opções deve ser implementada para atender aos requisitos da empresa? (Selecione DUAS.)

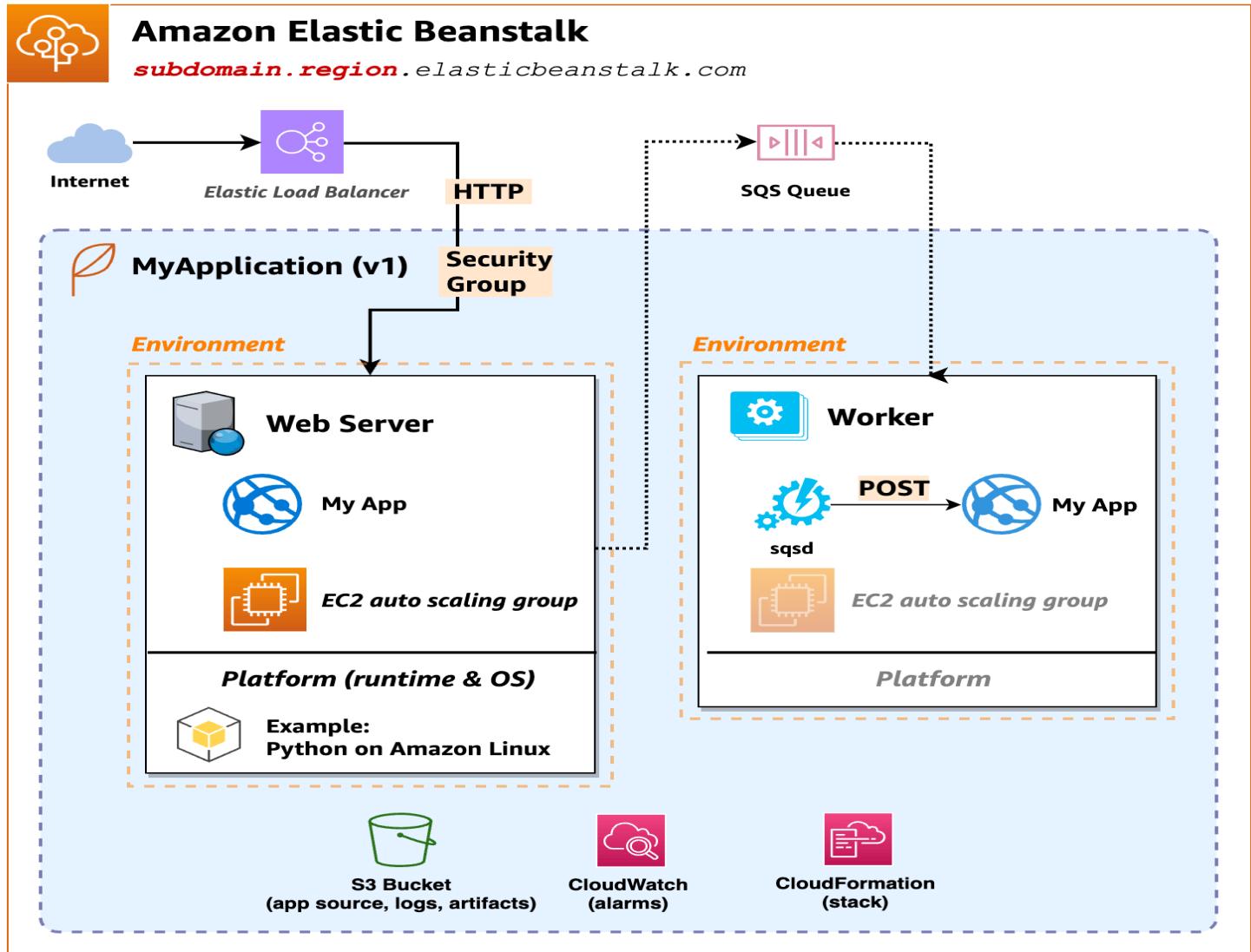
Rehospede o aplicativo .NET local em um ambiente AWS Elastic Beanstalk Multi-AZ que seja executado em várias Zonas de Disponibilidade.

Migre o banco de dados Oracle para o Amazon RDS para Oracle em uma implantação Multi-AZ usando o AWS Database Migration Service (AWS DMS).

O AWS Database Migration Service (AWS DMS) é um serviço de nuvem que facilita a migração de bancos de dados relacionais, data warehouses, bancos de dados NoSQL e outros tipos de armazenamento de dados. Você pode usar o AWS DMS para migrar seus dados para a Nuvem AWS ou entre combinações de nuvem e configurações locais.

Com o AWS DMS, você pode realizar migrações únicas e replicar alterações contínuas para manter as origens e os destinos sincronizados. Se quiser migrar para um mecanismo de banco de dados diferente, use a AWS Schema Conversion Tool (AWS SCT) para traduzir o esquema do seu banco de dados para a nova plataforma. Em seguida, use o AWS DMS para migrar os dados.

O **AWS Elastic Beanstalk** reduz a complexidade do gerenciamento sem restringir as opções ou o controle. Basta fazer o upload da sua aplicação e o Elastic Beanstalk cuida automaticamente dos detalhes de provisionamento de capacidade, balanceamento de carga, dimensionamento e monitoramento da integridade da aplicação. O Elastic Beanstalk oferece suporte a aplicações desenvolvidas em Go, Java, .NET, Node.js, PHP, Python e Ruby. Ao implantar sua aplicação, o Elastic Beanstalk cria a versão da plataforma compatível selecionada e provisiona um ou mais recursos da AWS, como instâncias do Amazon EC2, para executar sua aplicação.



O AWS Elastic Beanstalk para .NET facilita a implantação, o gerenciamento e o escalonamento de seus aplicativos web ASP.NET que utilizam a Amazon Web Services. O Elastic Beanstalk para .NET está disponível para qualquer pessoa que desenvolva ou hospede um aplicativo web que utilize o IIS.

Portanto, as respostas corretas são:

- Migrar o banco de dados Oracle para o Amazon RDS para Oracle em uma implantação Multi-AZ usando o AWS Database Migration Service (AWS DMS)
- Rehospede o aplicativo .NET local em um ambiente AWS Elastic Beanstalk Multi-AZ que é executado em várias zonas de disponibilidade.

A opção que diz: **Refatorar o aplicativo para .NET Core e executá-lo como um serviço de contêiner sem servidor usando o Amazon Elastic Kubernetes Service (Amazon EKS) com AWS Fargate** está incorreta. Isso exigirá alterações significativas no aplicativo, pois você refatorará ou alterará o código-base para

que ele se torne um aplicativo de contêiner sem servidor. Lembre-se de que o cenário mencionou explicitamente que o processo de migração deve minimizar as alterações de desenvolvimento. Uma solução melhor é simplesmente re-hospedar o aplicativo .NET local em um ambiente Multi-AZ do AWS Elastic Beanstalk, o que não requer nenhuma alteração de código.

A opção que diz: **Usar o AWS Application Migration Service (AWS MGN) para migrar o servidor de banco de dados Oracle local para uma nova instância do Amazon EC2** está incorreta. O Amazon RDS oferece suporte principalmente a bancos de dados Oracle padrão, portanto, seria melhor usar o AWS DMS para a migração do banco de dados, e não o AWS MGN.

A opção que diz: **Provisionar e replataformar o aplicativo para o Amazon Elastic Container Service (Amazon ECS) com nós de trabalho do Amazon EC2. Usar a Imagem de Máquina da Amazon (AMI) do Windows Server e implantar o aplicativo .NET usando-o no cluster ECS por meio do serviço ECS Anywhere** está incorreta. Isso pode ser possível, mas não recomendado para este cenário, pois você terá que gerenciar as instâncias EC2 subjacentes do seu cluster Amazon ECS que executarão o aplicativo. Seria melhor usar apenas o Elastic Beanstalk para cuidar do provisionamento dos recursos para o seu aplicativo .NET. Lembre-se de que realizar uma migração do tipo replataforma como esta envolve mudanças significativas no desenvolvimento, o que não é adequado aos requisitos fornecidos no cenário.

Referências:

<https://docs.aws.amazon.com/dms/latest/userguide>Welcome.html>

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/create_deploy_NET.html

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg>Welcome.html>

Confira estas folhas de dicas do AWS DMS e do AWS Beanstalk:

<https://tutorialsdojo.com/aws-database-migration-service/>

<https://tutorialsdojo.com/aws-elastic-beanstalk/>

38 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

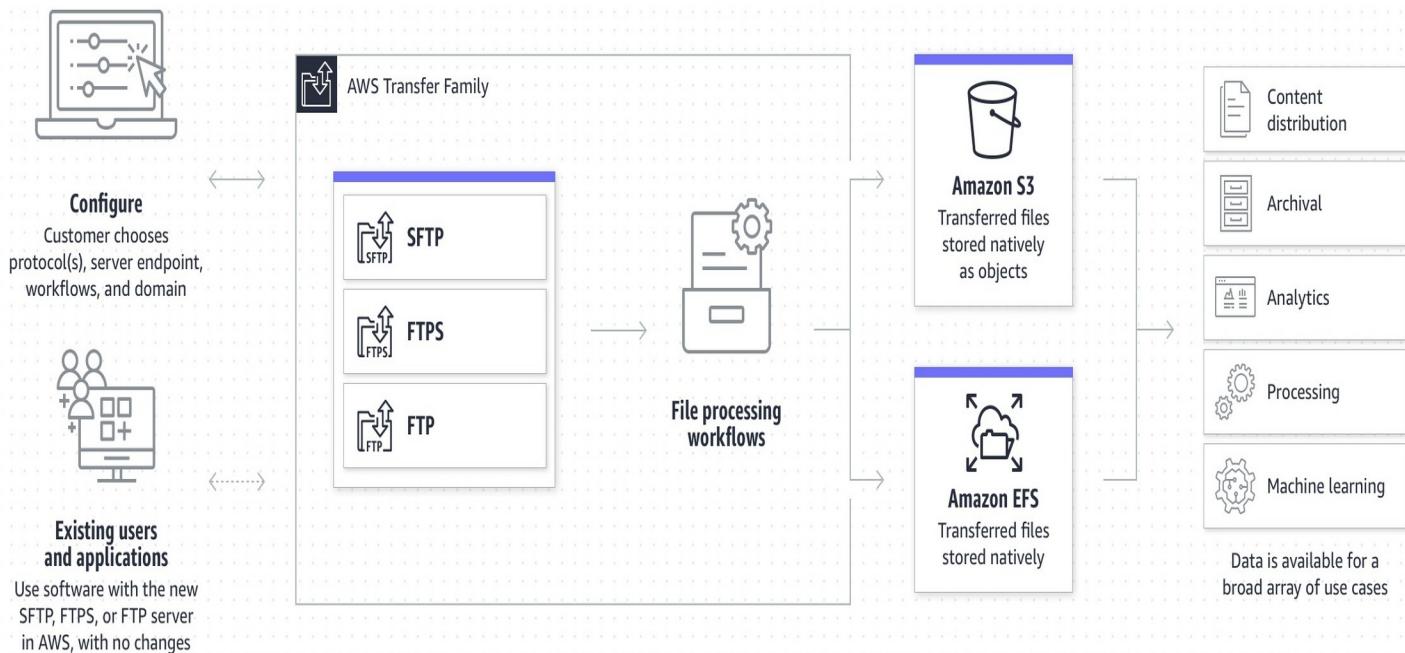
Uma empresa de logística planeja automatizar seu aplicativo de gerenciamento de pedidos. A empresa deseja usar a transferência de arquivos SFTP para enviar documentos críticos para os negócios. Como os arquivos são confidenciais, a criptografia em repouso é necessária e a alta disponibilidade deve ser garantida. Além disso, cada arquivo deve ser excluído automaticamente um mês após a criação.

Qual das seguintes opções deve ser implementada para atender aos requisitos da empresa com a menor sobrecarga operacional?

Crie um bucket do Amazon S3 com criptografia habilitada. Inicie um endpoint do AWS Transfer for SFTP para enviar arquivos com segurança para o bucket do S3. Configure uma regra de ciclo de vida do S3 para excluir arquivos após um mês.

O AWS Transfer for SFTP permite que você move facilmente suas cargas de trabalho de transferência de arquivos que usam o Secure Shell File Transfer Protocol (SFTP) para a AWS sem precisar modificar seus aplicativos ou gerenciar quaisquer servidores SFTP.

Para começar a usar o AWS Transfer for SFTP (AWS SFTP), crie um servidor SFTP e mapeie seu domínio para o endpoint do servidor, selecione a autenticação para seus clientes SFTP usando identidades gerenciadas pelo serviço ou integre seu próprio provedor de identidade e selecione seus buckets do Amazon S3 para armazenar os dados transferidos. Seus usuários atuais podem continuar operando com seus clientes ou aplicativos SFTP existentes. Os dados carregados ou baixados usando SFTP ficam disponíveis no seu bucket do Amazon S3 e podem ser usados para arquivamento ou processamento na AWS.



Uma configuração **de ciclo de vida do Amazon S3** é um conjunto de regras que definem ações que o Amazon S3 aplica a um grupo de objetos. Há dois tipos de ações:

Ações de transição - Essas ações definem quando os objetos são transferidos para outra classe de armazenamento. Por exemplo, você pode optar por transferir objetos para a classe de armazenamento S3 Standard-IA 30 dias após sua criação.

Ações de expiração - Essas ações definem quando os objetos expiram. O Amazon S3 exclui objetos expirados em seu nome.

Portanto, a resposta correta é: **Crie um bucket do Amazon S3 com criptografia habilitada. Inicie um endpoint do AWS Transfer for SFTP para enviar arquivos com segurança para o bucket do S3. Configure uma regra de ciclo de vida do S3 para excluir arquivos após um mês.** Você pode usar o S3 como serviço de armazenamento para seu servidor habilitado para AWS Transfer for SFTP.

A opção que diz: **Criar um bucket do Amazon S3 com criptografia habilitada. Configurar o AWS Transfer para SFTP para enviar arquivos com segurança para o bucket do S3. Configurar a política de retenção no servidor SFTP para excluir arquivos após um mês** está incorreta. A política de retenção de 30 dias deve ser configurada principalmente no bucket do Amazon S3. Não há opção de política de retenção no AWS Transfer para SFTP.

A opção que diz: **Criar um Amazon Elastic File System (Amazon EFS) e habilitar a criptografia. Configurar o AWS Transfer para SFTP para enviar arquivos com segurança para o sistema de arquivos EFS. Aplicar uma política de ciclo de vida do EFS para excluir arquivos após 30 dias** está incorreta. Isso pode ser possível, mas o gerenciamento do ciclo de vida do EFS não exclui objetos. Ele só permite a transição de arquivos para dentro e para fora da camada "Acesso Infrequente".

A opção que diz: **Provisionar uma instância do Amazon EC2 e instalar o serviço SFTP. Montar um sistema de arquivos criptografado do Amazon EFS na instância do EC2 para armazenar os arquivos enviados. Adicionar uma tarefa cron para excluir os arquivos com mais de um mês** está incorreta. Esta opção é possível, porém, acarreta uma sobrecarga operacional maior, pois você precisa gerenciar a instância do EC2 e o serviço SFTP.

Referências:

<https://aws.amazon.com/aws-transfer-family/>

<https://docs.aws.amazon.com/transfer/latest/userguide/create-server-sftp.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html>

Confira estas folhas de dicas do AWS Transfer Family e do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

<https://tutorialsdojo.com/aws-transfer-family/>

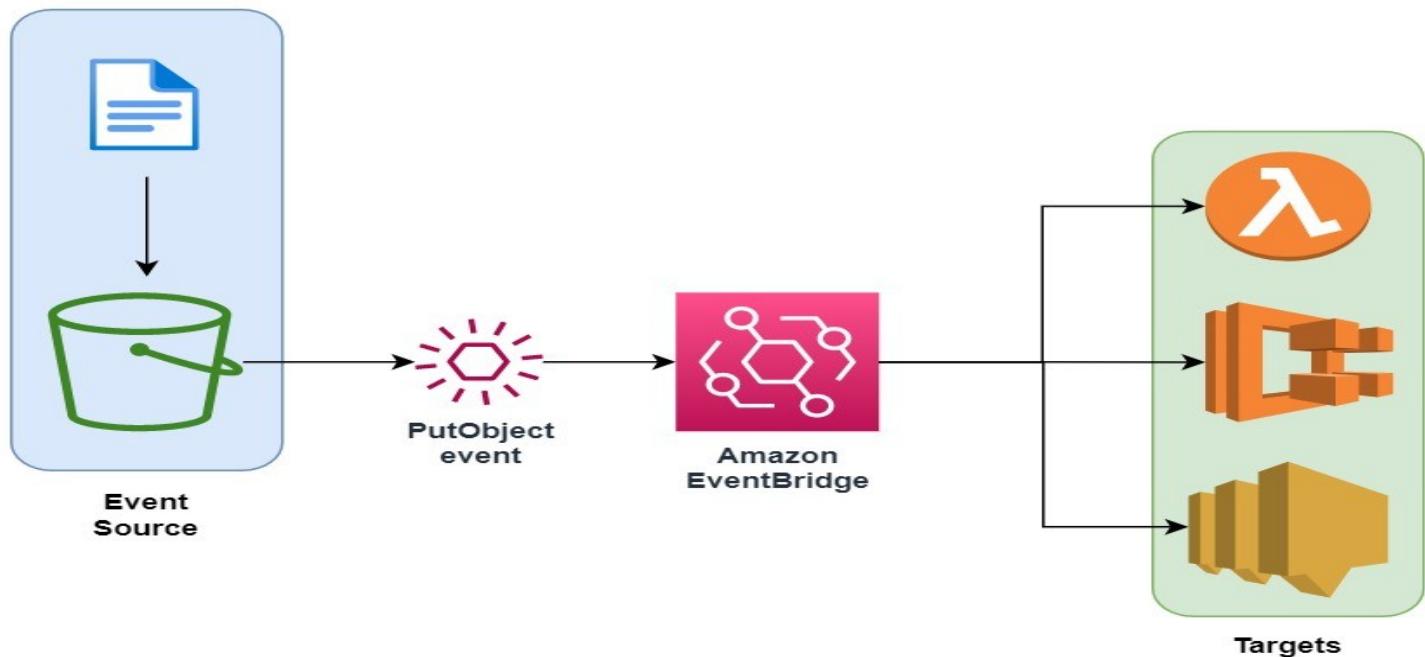
39 . Pergunta

Categoria: CSAA - Projeto de Arquiteturas Otimizadas em Custo

Uma empresa está usando o AWS Fargate para executar uma tarefa em lote sempre que um objeto é carregado em um bucket do Amazon S3. A contagem mínima de tarefas do ECS é inicialmente definida como 1 para economizar custos e só deve ser aumentada com base em novos objetos carregados no bucket do S3. Qual é a opção mais adequada para implementar com MENOR esforço?

Configure uma regra do Amazon EventBridge (Amazon CloudWatch Events) para detectar operações PUT de objetos do S3 e defina o destino para o cluster do ECS para executar uma nova tarefa do ECS.

O Amazon EventBridge (Amazon CloudWatch Events) é um barramento de eventos sem servidor que facilita a conexão de aplicativos. Ele utiliza dados dos seus próprios aplicativos, aplicativos integrados de software como serviço (SaaS) e serviços da AWS. Isso simplifica o processo de construção de arquiteturas orientadas a eventos, desacoplando produtores de eventos de consumidores de eventos. Isso permite que produtores e consumidores sejam escalados, atualizados e implantados de forma independente. O acoplamento flexível melhora a agilidade do desenvolvedor, além da resiliência do aplicativo.



Você pode usar o Amazon EventBridge (Amazon CloudWatch Events) para executar tarefas do Amazon ECS quando determinados eventos da AWS ocorrerem. Você pode configurar uma regra do EventBridge que execute uma tarefa do Amazon ECS sempre que um arquivo for carregado para um determinado bucket do Amazon S3 usando a operação PUT do Amazon S3.

Portanto, a resposta correta é: **configurar uma regra do Amazon EventBridge (Amazon CloudWatch Events) para detectar operações PUT de objetos do S3 e definir o destino para o cluster ECS para executar uma nova tarefa do ECS.**

A opção que diz: **Configurar uma regra do Amazon EventBridge (Amazon CloudWatch Events) para detectar operações PUT de objetos do S3 e definir o destino como uma função Lambda que executará o StartTask comando da API** está incorreta. Embora esta solução atenda ao requisito, criar sua própria função Lambda para este cenário não é realmente necessário. É muito mais simples controlar tarefas do

ECS diretamente como destinos para a regra de eventos do CloudWatch. Observe que o cenário solicita uma solução que seja a mais fácil de implementar.

A opção que diz: **Configurar um alarme no Amazon CloudWatch para monitorar operações em nível de objeto do S3 registradas no CloudTrail. Criar uma regra do Amazon EventBridge (Amazon CloudWatch Events) que acione o cluster do ECS quando novos eventos do CloudTrail forem detectados** está incorreta, pois usar o CloudTrail e o CloudWatch Alarm cria uma complexidade desnecessária para o que você deseja alcançar. O Amazon EventBridge (Amazon CloudWatch Events) pode direcionar diretamente uma tarefa do ECS na seção "Destinos" ao criar uma nova regra.

A opção que diz: **Configurar um alarme no CloudWatch para monitorar o CloudTrail, já que essas operações em nível de objeto do S3 são registradas no CloudTrail. Definir duas ações de alarme para atualizar a contagem de tarefas do ECS para escalar horizontalmente/horizontalmente dependendo do evento do S3** está incorreta, pois você não pode definir diretamente os Alarms do CloudWatch para atualizar a contagem de tarefas do ECS.

Referências:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-tutorial-ECS.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-Rule.html>

Confira esta folha de dicas do Amazon CloudWatch:

<https://tutorialsdojo.com/amazon-cloudwatch/>

40 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Uma empresa planeja migrar sua carga de trabalho local para a AWS. A arquitetura atual é composta por um servidor Microsoft SharePoint que utiliza um armazenamento de arquivos compartilhado do Windows. O Arquiteto de Soluções precisa usar uma solução de armazenamento em nuvem de alta disponibilidade e que possa ser integrada ao Active Directory para controle de acesso e autenticação.
Qual das seguintes opções pode satisfazer o requisito fornecido?

Crie um sistema de arquivos usando o Amazon FSx para Windows File Server e vincule-o a um domínio do Active Directory na AWS.

O Amazon FSx para Windows File Server oferece armazenamento de arquivos totalmente gerenciado, altamente confiável e escalável, acessível através do protocolo SMB (Service Message Block), padrão do setor. Ele é baseado no Windows Server e oferece uma ampla gama de recursos administrativos, como cotas de usuários, restauração de arquivos para usuários finais e integração com o Microsoft Active Directory (AD). O Amazon FSx pode ser acessado por meio de instâncias e dispositivos de computação Windows, Linux e MacOS. Milhares de instâncias e dispositivos de computação podem acessar um sistema de arquivos simultaneamente.

Windows authentication

Choose an Active Directory to provide user authentication and access control for your file system [Info](#)

AWS Managed Microsoft Active Directory

Self-managed Microsoft Active Directory

Choose an AWS Managed Microsoft AD directory to use. [Info](#)



[Create new directory](#)

O Amazon FSx funciona com o Microsoft Active Directory para integração com seus ambientes Microsoft Windows existentes. Você tem duas opções para fornecer autenticação de usuário e controle de acesso ao seu sistema de arquivos: o Microsoft Active Directory gerenciado pela AWS e o Microsoft Active Directory autogerenciado.

Observe que, após criar uma configuração do Active Directory para um sistema de arquivos, você não poderá alterá-la. No entanto, você pode criar um novo sistema de arquivos a partir de um backup e alterar a configuração de integração do Active Directory para esse sistema de arquivos. Essas configurações permitem que os usuários em seu domínio usem suas identidades existentes para acessar o sistema de arquivos do Amazon FSx e controlar o acesso a arquivos e pastas individuais.

Portanto, a resposta correta é: **Crie um sistema de arquivos usando o Amazon FSx for Windows File Server e vincule-o a um domínio do Active Directory na AWS.**

A opção que diz: **Criar um sistema de arquivos usando o Amazon EFS e vinculá-lo a um domínio do Active Directory** está incorreta porque o Amazon EFS não oferece suporte a sistemas Windows, apenas ao Linux. Você deve usar o Amazon FSx para Windows File Server para atender ao requisito do cenário.

A opção que diz: **Iniciar um Amazon EC2 Windows Server para montar um novo bucket do Amazon S3 como um volume de arquivo** está incorreta porque você não pode integrar o Amazon S3 ao seu Active Directory existente para fornecer autenticação e controle de acesso.

A opção que diz: **Criar um compartilhamento de arquivos do Sistema de Arquivos de Rede (NFS) usando o AWS Storage Gateway** está incorreta, pois o compartilhamento de arquivos NFS é usado principalmente para sistemas Linux. Lembre-se de que o requisito neste cenário é usar um armazenamento de arquivos compartilhado do Windows. Portanto, você deve usar um compartilhamento de arquivos SMB, que suporta o sistema operacional Windows e a configuração do Active Directory. Como alternativa, você também pode usar o sistema de arquivos do Amazon FSx para Windows File Server.

Referências:

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxw.html>

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html>

Confira esta folha de dicas do Amazon FSx:

<https://tutorialsdojo.com/amazon-fsx/>

41. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Um arquiteto de soluções precisa garantir que a instância do Amazon EC2 sob demanda só possa ser acessada a partir deste endereço IP (110.238.98.71) por meio de uma conexão SSH. Qual configuração abaixo atenderá a esse requisito?

Regra de entrada do grupo de segurança: Protocolo – TCP, Intervalo de portas – 22, Origem 110.238.98.71/32

Um **grupo de segurança** atua como um firewall virtual para sua instância, controlando o tráfego de entrada e saída. Ao iniciar uma instância em uma VPC, você pode atribuir até cinco grupos de segurança a ela. Os grupos de segurança atuam no nível da instância, não no nível da sub-rede. Portanto, cada instância em uma sub-rede da sua VPC pode ser atribuída a um conjunto diferente de grupos de segurança.

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>
HTTP	TCP	80	Custom <input type="button" value="▼"/> <input type="text" value="0.0.0.0/0"/> <input type="button" value="X"/>
HTTPS	TCP	443	Anywhere <input type="button" value="▼"/> <input type="text" value="0.0.0.0/0"/> <input type="button" value="X"/> ::/0 <input type="button" value="X"/>
SSH	TCP	22	Custom <input type="button" value="▼"/> <input type="text" value="110.238.98.71/32"/> <input type="button" value="X"/>

[Add rule](#)

O requisito é permitir apenas o IP individual do cliente e não a rede inteira. A notação CIDR /32 denota um único endereço IP. Observe que o protocolo SSH usa TCP, não UDP, e é executado na porta 22 (padrão). Nesse cenário, podemos criar um grupo de segurança com uma regra de entrada permitindo o tráfego de entrada do endereço IP especificado na porta 22.

Os grupos de segurança são stateful, o que significa que permitem automaticamente o tráfego de retorno associado ao cliente que iniciou a conexão com a instância. Portanto, qualquer tráfego de retorno do endereço IP especificado na porta 22 poderá passar pelo grupo de segurança, independentemente de haver ou não uma regra de saída explícita que o permita.

Portanto, a resposta correta é: **Regra de entrada do grupo de segurança: Protocolo - TCP, Intervalo de portas - 22, Origem 110.238.98.71/32**

A opção que diz: **Regra de entrada do grupo de segurança: Protocolo - UDP, Intervalo de portas - 22, Origem 110.238.98.71/32** está incorreta porque normalmente usa UDP em vez de TCP. O SSH é executado sobre o protocolo TCP, portanto, especificar UDP não permitiria o acesso desejado.

A opção que diz: **Regra de Saída do Grupo de Segurança: Protocolo - TCP, Intervalo de Portas - 22, Destino 110.238.98.71/32** está incorreta porque é uma regra de saída, não de entrada. As regras de saída controlam o tráfego que sai da instância. Neste cenário, precisamos limitar o tráfego de entrada proveniente de um endereço específico.

A opção que diz: **Regra de Saída do Grupo de Segurança: Protocolo - UDP, Intervalo de Portas - 22, Destino 0.0.0.0/0** está incorreta porque é uma regra de saída e não de entrada. Além disso, conexões SSH requerem apenas TCP.

Referências:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-group-rules>

<https://docs.aws.amazon.com/vpc/>

Guia de estudo para o exame AWS Certified Solutions Architect Associate da Tutoriais Dojo:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate/>

Confira esta folha de dicas do Amazon EC2:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

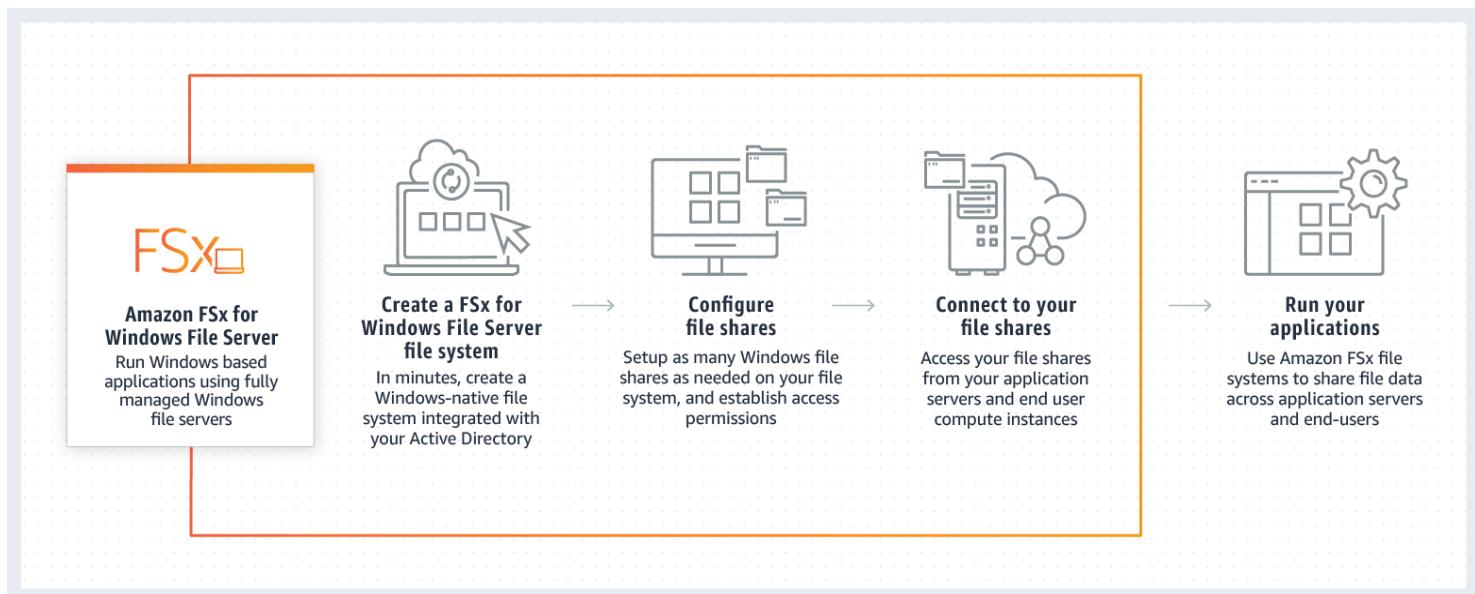
42 . PREGUNTA

Categoría: CSAA - Design de Arquiteturas de Alto Desempenho

Uma empresa possui um aplicativo web que utiliza os Serviços de Informações da Internet (IIS) para Windows Server. Um compartilhamento de arquivos é usado para armazenar os dados do aplicativo no armazenamento conectado à rede do data center local da empresa. Para obter um sistema de alta disponibilidade, a empresa planeja migrar o aplicativo e o compartilhamento de arquivos para a AWS. Qual das seguintes opções pode ser usada para atender a esse requisito?

Migre a configuração de compartilhamento de arquivos existente para o Amazon FSx para Windows File Server.

O Amazon FSx for Windows File Server oferece servidores de arquivos Microsoft Windows totalmente gerenciados, apoiados por um sistema de arquivos Windows totalmente nativo. O Amazon FSx for Windows File Server possui os recursos, o desempenho e a compatibilidade para migrar e migrar facilmente aplicativos corporativos para a Nuvem AWS. Ele pode ser acessado a partir de instâncias e dispositivos de computação Windows, Linux e macOS. Milhares de instâncias e dispositivos de computação podem acessar um sistema de arquivos simultaneamente.



Neste cenário, você precisa migrar sua configuração de compartilhamento de arquivos existente para a nuvem. Dentre as opções apresentadas, a melhor resposta possível é o Amazon FSx. Um compartilhamento de arquivos é uma pasta específica no seu sistema de arquivos, incluindo as subpastas da pasta, que você torna acessível às suas instâncias de computação por meio do protocolo SMB. Para migrar as configurações de compartilhamento de arquivos do seu sistema de arquivos local, você deve migrar seus arquivos primeiro para o Amazon FSx antes de migrar sua configuração de compartilhamento de arquivos.

Portanto, a resposta correta é: **migre a configuração de compartilhamento de arquivos existente para o Amazon FSx para Windows File Server**.

A opção que diz: **Migrar a configuração de compartilhamento de arquivos existente para o AWS Storage Gateway** está incorreta porque o AWS Storage Gateway é usado principalmente para integrar sua rede local à AWS, mas não para migrar seus aplicativos. Usar um compartilhamento de arquivos no Storage Gateway implica que você ainda manterá seus sistemas locais, e não os migrará completamente.

A opção que diz: **Migrar a configuração de compartilhamento de arquivos existente para o Amazon EFS** está incorreta, pois consta no cenário que a empresa está usando um compartilhamento de arquivos executado em um servidor Windows. Lembre-se de que o Amazon EFS oferece suporte apenas a cargas de trabalho Linux.

A opção que diz: **Migrar a configuração de compartilhamento de arquivos existente para o Amazon EBS** está incorreta porque o EBS é usado principalmente como armazenamento em bloco para instâncias do

EC2 e não como um sistema de arquivos compartilhado. Um compartilhamento de arquivos é uma pasta específica em um sistema de arquivos que você pode acessar usando um protocolo SMB (Server Message Block). O Amazon EBS não oferece suporte ao protocolo SMB.

Referências:

<https://aws.amazon.com/fsx/windows/faqs/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-file-share-config-to-fsx.html>

Confira esta folha de dicas do Amazon FSx:

<https://tutorialsdojo.com/amazon-fsx/>

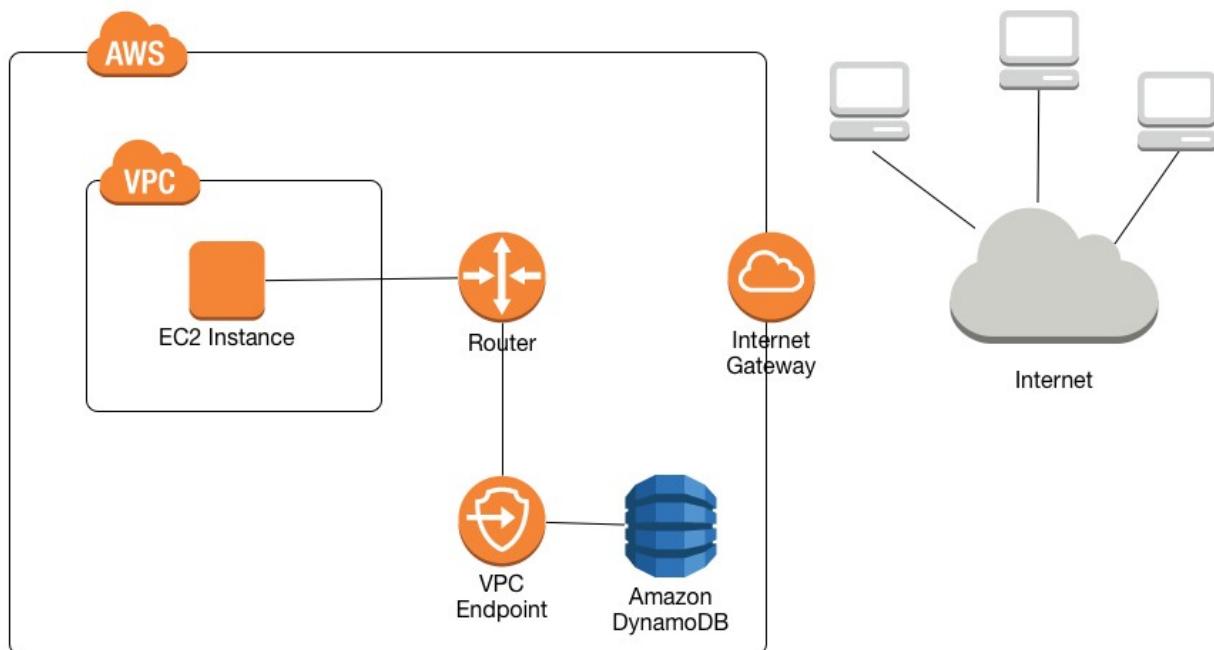
43 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa planeja lançar uma instância do Amazon EC2 em uma sub-rede privada para seu portal corporativo interno. Por motivos de segurança, a instância do EC2 deve enviar dados para o Amazon DynamoDB e o Amazon S3 por meio de endpoints privados que não passam pela internet pública. Qual das seguintes opções pode atender aos requisitos acima?

Use endpoints do Amazon VPC para rotear todo o acesso ao S3 e ao DynamoDB por meio de endpoints privados.

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



No cenário, você é solicitado a configurar endpoints privados para enviar dados ao Amazon DynamoDB e ao Amazon S3 sem acessar a internet pública. Dentre as opções oferecidas, o endpoint VPC é o serviço mais adequado, permitindo que você use endereços IP privados para acessar o DynamoDB e o S3 sem qualquer exposição à internet pública.

Portanto, a resposta correta é: **use endpoints do Amazon VPC para rotear todo o acesso ao S3 e ao DynamoDB por meio de endpoints privados.**

A opção que diz: **Habilitar a Criptografia em Repouso do DynamoDB com a chave padrão gerenciada pela AWS e a Criptografia do Lado do Servidor S3 com a chave padrão do AWS KMS para rotear todo o tráfego para o DynamoDB e o S3 por meio de endpoints privados** está incorreta porque a criptografia em repouso não afeta o roteamento do tráfego. A criptografia gerencia a segurança dos dados, mas não controla como o tráfego é roteado entre os serviços.

A opção que diz: **Usar o AWS Direct Connect para rotear todo o acesso ao S3 e ao DynamoDB por meio de endpoints privados** está incorreta, pois o AWS Direct Connect é usado principalmente para estabelecer uma conexão de rede dedicada das suas instalações para a AWS. O cenário não indica que a empresa está usando seu servidor local ou que possui uma arquitetura de nuvem híbrida.

A opção que diz: **Usar o AWS VPN CloudHub para rotear todo o acesso no S3 e no DynamoDB para um endpoint privado** está incorreta porque o AWS VPN CloudHub normalmente é usado para fornecer comunicação segura entre sites remotos e não para criar um endpoint privado para acessar o Amazon S3 e o DynamoDB dentro da rede da Amazon.

Referências:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

<https://docs.aws.amazon.com/glue/latest/dg/vpc-endpoints-s3.html>

Confira esta folha de dicas do Amazon VPC:

<https://tutorialsdojo.com/amazon-vpc/>

44 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma empresa conta com 3 engenheiros de DevOps responsáveis pelos processos de desenvolvimento de software e gerenciamento de infraestrutura. Um dos engenheiros excluiu acidentalmente um arquivo hospedado no Amazon S3, o que causou a interrupção do serviço.

O que os engenheiros de DevOps podem fazer para evitar que isso aconteça novamente?

Habilite o controle de versão do S3 e a exclusão da autenticação multifator no bucket.

Para aprimorar a proteção de dados e atender às práticas recomendadas de segurança de objetos armazenados, a AWS recomenda implementar proteções contra exclusões acidentais. Para evitar exclusões acidentais em um bucket do Amazon S3, você pode:

- Habilitar controle de versão
- Habilitar MFA (Autenticação Multifator) Excluir

S | Search [Alt+S] | Asia Pacific (Singapore) ▾ lualhati.bautista @ tutorialsdojo ▾

Amazon S3 > Buckets > tutorialsdojo-laguna > Edit Bucket Versioning

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight

Edit Bucket Versioning

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

[Cancel](#) [Save changes](#)

O **versionamento** é um meio de manter múltiplas variantes de um objeto no mesmo bucket. Você pode usar o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no seu bucket do Amazon S3. Com o versionamento, você pode se recuperar facilmente de ações não intencionais do usuário e de falhas no aplicativo.

▼ Using the AWS CLI

The following example enables S3 Versioning and multi-factor authentication (MFA) delete on a bucket.

```
aws s3api put-bucket-versioning --bucket DOC-EXAMPLE-BUCKET1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

Se a **exclusão de MFA (autenticação multifator)** estiver habilitada, será necessária autenticação adicional para qualquer uma das seguintes operações:

- Alterar o estado de versionamento do seu bucket
- Excluir permanentemente uma versão do objeto

Portanto, a resposta correta é: **Habilitar o controle de versão do S3 e a exclusão da autenticação multifator no bucket.**

Usar o armazenamento S3 de Acesso Infrequente para armazenar os dados é . Alterar sua classe de armazenamento para S3 de Acesso Infrequente não ajudará a mitigar exclusões acidentais.

Configurar uma URL assinada para todos os usuários é . URLs assinadas oferecem mais controle sobre o acesso ao seu conteúdo, portanto, esse recurso se concentra mais no acesso do que na exclusão.

Criar uma política de bucket do IAM que desabilite a operação de exclusão é . Se você criar uma política de bucket que impeça a exclusão, outros usuários não poderão excluir objetos que deveriam ser excluídos. Você só quer evitar a exclusão acidental, não desabilitar a ação em si.

Referências:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

45 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma empresa utiliza um Application Load Balancer (ALB) para suas aplicações web multicamadas públicas. A equipe de segurança relatou recentemente que houve um aumento repentino de ataques de injeção de SQL, o que causa problemas críticos de discrepância de dados. O mesmo problema também é encontrado por suas outras aplicações web em outras contas da AWS que estão por trás de um ALB. Uma solução imediata é necessária para impedir a injeção remota de consultas SQL não autorizadas e proteger suas aplicações hospedadas em várias contas.

Como arquiteto de soluções, qual solução você recomendaria?

Use o AWS WAF e configure uma regra gerenciada para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Associe-a ao Application Load Balancer. Integre o AWS WAF ao AWS Firewall Manager para reutilizar as regras em todas as contas da AWS.

O AWS WAF é um firewall de aplicativo da Web que permite monitorar as solicitações HTTP(S) encaminhadas para uma distribuição do Amazon CloudFront, uma API REST do Amazon API Gateway, um平衡ador de carga de aplicativo ou uma API GraphQL do AWS AppSync.

- **ACLs da Web** - Use uma lista de controle de acesso (ACL) da Web para proteger um conjunto de recursos da AWS. Crie uma ACL da Web e defina sua estratégia de proteção adicionando regras. As regras definem critérios para inspecionar solicitações da Web e especificam como lidar com as solicitações que correspondem a esses critérios. Defina uma ação padrão para a ACL da Web que indica se as solicitações que passam nas inspeções das regras devem ser bloqueadas ou permitidas.

Regras - Cada regra contém uma instrução que define os critérios de inspeção e uma ação a ser tomada caso uma solicitação da web atenda aos critérios. Quando uma solicitação da web atende aos critérios, isso significa que houve uma correspondência. Você pode configurar regras para bloquear solicitações correspondentes, permitir a passagem, contá-las ou executar controles CAPTCHA nelas.

Grupos de regras - Você pode usar regras individualmente ou em grupos de regras reutilizáveis. As Regras Gerenciadas da AWS e os vendedores do AWS Marketplace fornecem grupos de regras gerenciadas para você usar. Você também pode definir seus próprios grupos de regras.

AWSManagedRulesSQLiRuleSet - O grupo de regras do banco de dados SQL contém regras para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Isso pode ajudar a prevenir a injeção remota de consultas não autorizadas. Avalie este grupo de regras para uso se o seu aplicativo interagir com um banco de dados SQL.

Serviços | Search for services, features, blogs, docs, and more [Option+S] Global ▾ Tutorials Dojo ▾

WAF & Shield X AWS WAF > Web ACLs > Create web ACL

Step 1: Describe web ACL and associate it to AWS resources

Step 2: Add rules and rule groups: Add managed rule groups

Step 3: Set rule priority

Step 4: Configure metrics

Step 5: Review and create web ACL

Add managed rule groups [Info](#) Close

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers.

▼ AWS managed rule groups

Paid rule groups

Name	Capacity	Action
Account takeover prevention	50	<input type="radio"/> Add to web ACL
Bot Control	50	<input type="radio"/> Add to web ACL

Rule Group to prevent SQL Injection Attacks

Free rule groups

Name	Capacity	Action
SQL database	200	<input type="radio"/> Add to web ACL
Admin protection	100	<input type="radio"/> Add to web ACL

TD TUTORIALS DO JOO

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

O AWS WAF é fácil de implantar e proteger aplicativos implantados no Amazon CloudFront como parte da sua solução de CDN, no Application Load Balancer que gerencia todos os seus servidores de origem, no Amazon API Gateway para suas APIs REST ou no AWS AppSync para suas APIs GraphQL. Não há necessidade de software adicional para implantar, configuração de DNS, gerenciamento de certificado SSL/TLS ou configuração de proxy reverso.

Com a integração do AWS Firewall Manager, você pode definir e gerenciar centralmente suas regras e reutilizá-las em todos os aplicativos da Web que você precisa proteger.

Portanto, a resposta correta é: **use o AWS WAF e configure uma regra gerenciada para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Associe-a ao Application Load Balancer. Integre o AWS WAF ao AWS Firewall Manager para reutilizar as regras em todas as contas da AWS.**

A opção que diz: **Usar o Amazon GuardDuty e configurar uma regra gerenciada para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Associar ao Application Load Balancer e utilizar o serviço AWS Security Hub para reutilizar as regras gerenciadas em todas as contas da AWS** está incorreta, pois o Amazon GuardDuty é apenas um serviço de detecção de ameaças e não pode ser integrado diretamente ao Application Load Balancer.

A opção que diz: **Use o AWS Network Firewall para filtrar vulnerabilidades da web e ataques de força bruta usando grupos de regras com estado em todos os Application Load Balancers em todas as contas da AWS. Refatorar o aplicativo web para torná-lo menos suscetível a ataques de injeção de SQL com base na avaliação de segurança** está incorreta, pois o AWS Network Firewall é um serviço gerenciado usado principalmente para implantar proteções de rede essenciais para todas as suas Amazon Virtual Private Clouds (VPCs) e não especificamente para seus Application Load Balancers. Observe que o AWS Network Firewall é específico da conta por padrão e precisa ser integrado ao AWS Firewall Manager para compartilhar facilmente o firewall entre suas outras contas da AWS. Além disso, refatorar o aplicativo web exigirá muito tempo.

As opções que dizem: **Usar o Amazon Macie para verificar vulnerabilidades e exposição não intencional da rede. Refatorar o aplicativo web para torná-lo menos suscetível a ataques de injeção de SQL com base na avaliação de segurança. Utilizar o AWS Audit Manager para reutilizar a avaliação de segurança em todas as contas da AWS** está porque o Amazon Macie é usado apenas para serviços de segurança e privacidade de dados que utilizam aprendizado de máquina e correspondência de padrões para descobrir e proteger seus dados confidenciais. Assim como antes, refatorar o aplicativo web exigirá uma quantidade imensa de tempo. O uso do AWS Audit Manager também não é relevante. O AWS Audit Manager simplesmente ajuda você a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia riscos e a conformidade com regulamentações e padrões do setor.

Referências:

<https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html#aws-managed-rule-groups-use-case-sql-db>

Confira esta folha de dicas do AWS Web Application Firewall:

<https://tutorialsdojo.com/aws-waf>

46. PERGUNTA

Categoria: CSAA – Projeto de Arquiteturas Otimizadas em Custo

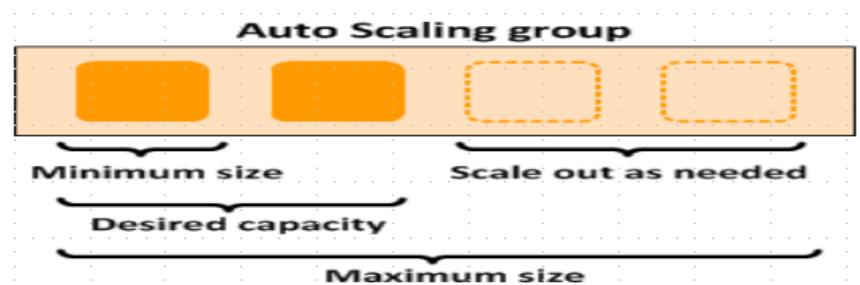
Uma empresa hospedou uma aplicação web em um grupo de instâncias EC2 de Auto Scaling. O gerente de TI está preocupado com o excesso de provisionamento de recursos, que pode gerar custos operacionais mais altos. Um Arquiteto de Soluções foi instruído a criar uma solução econômica sem afetar o desempenho da aplicação.

Qual política de dimensionamento dinâmico deve ser usada para atender a esse requisito?

Use a escala de rastreamento de destino.

Um grupo de Auto Scaling contém uma coleção de instâncias do Amazon EC2 que são tratadas como um agrupamento lógico para fins de dimensionamento e gerenciamento automáticos. Um grupo de Auto Scaling também permite que você use os recursos do Amazon EC2 Auto Scaling, como substituições de verificações de integridade e políticas de dimensionamento. Tanto a manutenção do número de instâncias em um grupo de Auto Scaling quanto o dimensionamento automático são as principais funcionalidades do serviço Amazon EC2 Auto Scaling. O tamanho de um grupo de Auto Scaling depende do número de instâncias definido como a capacidade desejada. Você pode ajustar seu tamanho para atender à demanda, manualmente ou usando o dimensionamento automático.

Políticas de escalonamento em etapas e políticas de escalonamento simples são duas das opções de escalonamento dinâmico disponíveis. Ambas exigem a criação de alarmes do CloudWatch para as políticas de escalonamento. Ambas exigem a especificação dos limites alto e baixo para os alarmes. Ambas exigem que você defina se deseja adicionar ou remover instâncias, e quantas, ou definir o grupo para um tamanho exato. A principal diferença entre os tipos de política são os ajustes em etapas obtidos com as políticas de escalonamento em etapas. Quando os ajustes em etapas são aplicados e aumentam ou diminuem a capacidade atual do seu grupo de Dimensionamento Automático, os ajustes variam de acordo com o tamanho da violação de alarme.



O principal problema com o escalonamento simples é que, após o início de uma atividade de escalonamento, a política precisa aguardar a conclusão da atividade de escalonamento ou a substituição da verificação de integridade e o término do período de espera antes de responder a alarmes adicionais. Os períodos de espera ajudam a evitar o início de atividades de escalonamento adicionais antes que os efeitos das atividades anteriores sejam visíveis.

Com uma política de escalonamento com acompanhamento de metas, você pode aumentar ou diminuir a capacidade atual do grupo com base em um valor-alvo para uma métrica específica. Essa política ajudará a resolver o excesso de provisionamento dos seus recursos. A política de escalonamento adiciona ou remove capacidade conforme necessário para manter a métrica no valor-alvo especificado ou próximo a ele. Além de manter a métrica próxima ao valor-alvo, uma política de escalonamento com acompanhamento de metas também se ajusta às alterações na métrica devido a um padrão de carga variável.

Portanto, a resposta correta é: **usar escala de rastreamento de destino**.

A opção que diz: **Usar escalonamento simples** está incorreta porque você precisa aguardar a conclusão do período de espera antes de iniciar atividades de escalonamento adicionais. Políticas de rastreamento de metas ou escalonamento em etapas podem acionar uma atividade de escalonamento imediatamente, sem aguardar o término do período de espera.

A opção que diz: **Usar escalonamento agendado** está incorreta porque esta política é usada principalmente para padrões de tráfego previsíveis. Você precisa usar a política de escalonamento de rastreamento de destino para otimizar o custo da sua infraestrutura sem afetar o desempenho.

A opção que diz: **Usar suspensão e retomada de dimensionamento** está incorreta porque esse tipo é usado para pausar temporariamente atividades de dimensionamento acionadas por suas políticas de dimensionamento e ações agendadas.

Referências:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

Confira esta folha de dicas de dimensionamento automático da AWS:

<https://tutorialsdojo.com/aws-auto-scaling/>

47 . Pergunta

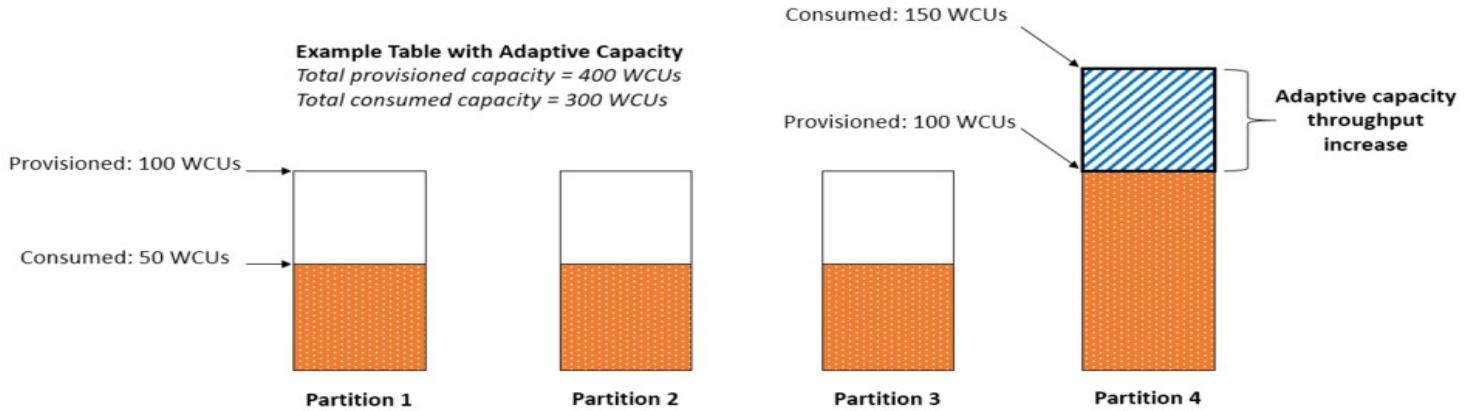
Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Um aplicativo Docker, executado em um cluster do Amazon ECS por trás de um平衡ador de carga, utiliza intensamente o Amazon DynamoDB. O aplicativo precisa melhorar o desempenho do banco de dados, distribuindo a carga de trabalho uniformemente e utilizando a taxa de transferência provisionada de forma eficiente.

Qual das seguintes opções deve ser implementada para a tabela do DynamoDB?

Use chaves de partição com atributos de alta cardinalidade, que tenham um grande número de valores distintos para cada item.

A parte da chave de partição da chave primária de uma tabela determina as partições lógicas nas quais os dados da tabela são armazenados. Isso, por sua vez, afeta as partições físicas subjacentes. A capacidade de E/S provisionada para a tabela é dividida igualmente entre essas partições físicas. Portanto, um design de chave de partição que não distribui as solicitações de E/S uniformemente pode criar partições "quentes", resultando em limitação de tráfego e usando sua capacidade de E/S provisionada de forma ineficiente.



O uso ideal do throughput provisionado de uma tabela depende não apenas dos padrões de carga de trabalho de itens individuais, mas também do design da chave de partição. Isso não significa que você precisa acessar todos os valores de chave de partição para atingir um nível de throughput eficiente, ou mesmo que a porcentagem de valores de chave de partição acessados precisa ser alta. Significa que quanto mais valores de chave de partição distintos sua carga de trabalho acessa, mais essas solicitações serão distribuídas pelo espaço particionado. Em geral, você usará seu throughput provisionado com mais eficiência à medida que a proporção de valores de chave de partição acessados em relação ao número total de valores de chave de partição aumenta.

Portanto, a resposta correta é: **Use chaves de partição com atributos de alta cardinalidade, que tenham um grande número de valores distintos para cada item**.

A opção que diz: **Reducir o número de chaves de partição na tabela do DynamoDB** está incorreta. Em vez de fazer isso, você deveria adicionar mais para melhorar o desempenho e distribuir as solicitações de E/S uniformemente, e não simplesmente evitar partições "quentes".

A opção que diz: **Usar chaves de partição com atributos de baixa cardinalidade, que possuem poucos valores distintos para cada item**, está incorreta porque é exatamente o oposto da resposta correta. Lembre-se de que quanto mais valores distintos de chaves de partição sua carga de trabalho acessa, mais essas solicitações serão distribuídas pelo espaço particionado. Por outro lado, quanto menos valores distintos de chaves de partição, menos uniformemente distribuídas elas serão pelo espaço particionado, o que efetivamente reduz o desempenho.

A opção que diz: **Evite usar uma chave primária composta, que é composta por uma chave de partição e uma chave de classificação**, está incorreta porque, como mencionado, uma chave primária composta fornecerá mais partição para a tabela e, por sua vez, melhorará o desempenho. Portanto, ela deve ser usada e não evitada.

Referências:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-uniform-load.html>

<https://aws.amazon.com/blogs/database/choosing-the-right-dynamodb-partition-key/>

Confira esta folha de dicas do Amazon DynamoDB:

<https://tutorialsdojo.com/amazon-dynamodb/>

Visão geral do Amazon DynamoDB:

48 . PREGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Uma aplicação financeira consiste em um grupo de Auto Scaling de instâncias do Amazon EC2, um Application Load Balancer e uma instância do MySQL RDS configurada em uma configuração de implantação

Multi-AZ. Para proteger os dados confidenciais dos clientes, é necessário garantir que o banco de dados do Amazon RDS seja acessível somente por meio de um token de autenticação específico para as credenciais de perfil das instâncias do EC2.

Qual das seguintes ações deve ser tomada para atender a esse requisito?

Habilite a autenticação do IAM DB.

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

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

Database options

DB cluster identifier [Info](#)
tutorialsdojo
If you do not provide one, a default identifier based on the instance identifier will be used.

Database name [Info](#)
tutorialsdojo
If you do not specify a database name, Amazon RDS does not create a database.

Port [Info](#)
TCP/IP port the DB instance will use for application connections.
3306

DB parameter group [Info](#)
default.aurora5.6

DB cluster parameter group [Info](#)
default.aurora5.6

Option group [Info](#)
default:aurora-5-6

IAM DB authentication [Info](#)
 Enable IAM DB authentication
Manage your database user credentials through AWS IAM users and roles.
 Disable

A autenticação do banco de dados IAM oferece os seguintes benefícios:

- O tráfego de rede de e para o banco de dados é criptografado usando Secure Sockets Layer (SSL).
- Você pode usar o IAM para gerenciar centralmente o acesso aos recursos do seu banco de dados, em vez de gerenciar o acesso individualmente em cada instância do banco de dados.

Para aplicativos em execução no Amazon EC2, você pode usar credenciais de perfil específicas para sua instância do EC2 para acessar seu banco de dados em vez de uma senha, para maior segurança. Portanto, a resposta correta é: **Habilitar a autenticação do IAM DB**.

A opção que diz: **Configurar SSL no seu aplicativo para criptografar a conexão do banco de dados com o RDS** está incorreta porque uma conexão SSL não utiliza apenas um token de autenticação do IAM. Embora configurar SSL no seu aplicativo possa melhorar a segurança dos seus dados em trânsito, ainda não é uma opção adequada para usar neste cenário.

A opção que diz: **Criar uma função do IAM e atribuí-la às suas instâncias do EC2, que concederão acesso exclusivo à sua instância do RDS**, está incorreta porque, embora você possa criar e atribuir uma função do IAM às suas instâncias do EC2, ainda precisa configurar seu RDS para usar a autenticação do banco de dados do IAM.

A opção que diz: **Usar uma combinação de IAM e STS para impor acesso restrito à sua instância do RDS usando um token de autenticação temporário** está incorreta, pois você precisa usar a Autenticação de Banco de Dados do IAM para este cenário, e não simplesmente uma combinação de IAM e STS. Embora o STS seja usado para enviar tokens temporários para autenticação, este não é um caso de uso compatível para o RDS.

Referências:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

<https://aws.amazon.com/rds/>

Confira esta folha de dicas do Amazon RDS:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

49 . Pergunta

Categoria: CSAA - Design de Arquiteturas Resilientes

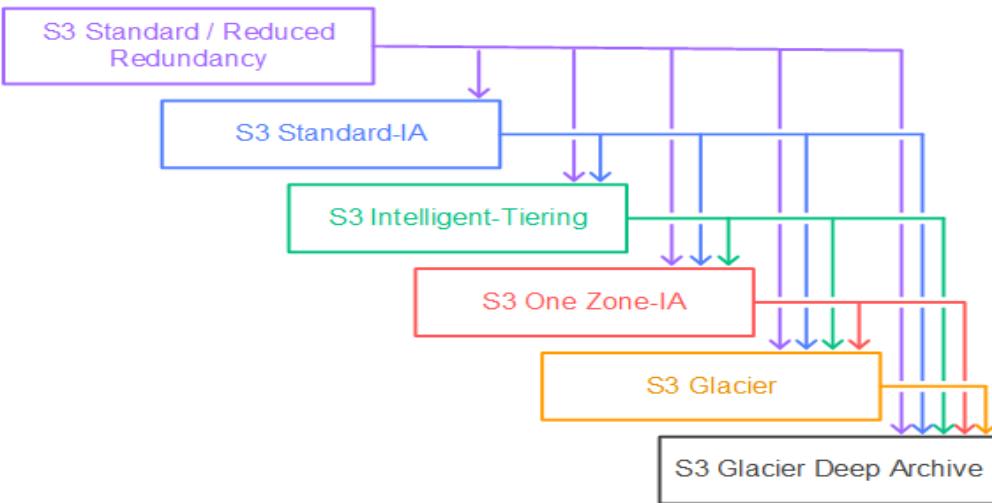
Uma empresa planeja hospedar uma aplicação web em um grupo de Auto Scaling de instâncias do Amazon EC2. A aplicação será usada globalmente por usuários para carregar e armazenar diversos tipos de arquivos. Com base nas tendências dos usuários, arquivos com mais de 2 anos devem ser armazenados em uma classe de armazenamento diferente. O Arquiteto de Soluções da empresa precisa criar uma solução econômica e escalável para armazenar os arquivos antigos, mas que ainda ofereça durabilidade e alta disponibilidade.

Qual das seguintes abordagens pode ser usada para atender a esse requisito? (Selecione DUAS.)

Use o Amazon S3 e crie uma política de ciclo de vida que moverá os objetos para o Amazon S3 Glacier após 2 anos.

Use o Amazon S3 e crie uma política de ciclo de vida que moverá os objetos para o Amazon S3 Standard-IA após 2 anos.

O Amazon S3 armazena dados como objetos em buckets. Um objeto é um arquivo e quaisquer metadados opcionais que o descrevam. Para armazenar um arquivo no Amazon S3, carregue-o em um bucket. Ao carregar um arquivo como um objeto, você pode definir permissões para o objeto e quaisquer metadados. Buckets são contêineres para objetos. Você pode ter um ou mais buckets. Você pode controlar o acesso a cada bucket, decidindo quem pode criar, excluir e listar objetos nele. Você também pode escolher a região geográfica onde o Amazon S3 armazenará o bucket e seu conteúdo e visualizar os logs de acesso do bucket e seus objetos.



Para mover um arquivo para uma classe de armazenamento diferente, você pode usar o Amazon S3 ou o Amazon EFS. Ambos os serviços possuem configurações de ciclo de vida. Observe que o Amazon EFS só pode transferir um arquivo para a classe de armazenamento IA após 90 dias. Como você precisa mover os arquivos com mais de 2 anos para uma solução mais econômica e escalável, use a configuração de ciclo de vida do Amazon S3. Com as regras de ciclo de vida do S3, você pode transferir arquivos para o S3 Standard IA ou o S3 Glacier. Usando a recuperação rápida do S3 Glacier, você pode acessar seus arquivos rapidamente em 1 a 5 minutos.

Portanto, as respostas corretas são:

- Use o Amazon S3 e crie uma política de ciclo de vida que moverá os objetos para o Amazon S3 Glacier após 2 anos.
- Use o Amazon S3 e crie uma política de ciclo de vida que moverá os objetos para o Amazon Standard-IA após 2 anos.

A opção que diz: **Usar o Amazon EFS e criar uma política de ciclo de vida que moverá os objetos para o Amazon EFS-IA após 2 anos** está incorreta porque o máximo de dias das políticas de ciclo de vida do EFS é de apenas 365 dias. Portanto, ela ainda não atende ao requisito de mover arquivos com mais de 2 anos ou 730 dias.

A opção que diz: **Usar volumes do Amazon EBS para armazenar os arquivos. Configurar o Amazon Data Lifecycle Manager (DLM) para agendar snapshots dos volumes após 2 anos** está incorreta porque o Amazon EBS simplesmente custa mais e não é tão escalável quanto o Amazon S3. Ele tem algumas limitações quando acessado por várias instâncias do EC2. Também há custos elevados envolvidos no uso do recurso de multianexação em um volume do EBS com IOPS provisionadas para permitir que várias instâncias do EC2 acessem o volume.

A opção que diz: **Usar uma configuração de armazenamento RAID 0 que distribui vários volumes do Amazon EBS para armazenar os arquivos. Configurar o Gerenciador de Ciclo de Vida de Dados (DLM) da Amazon para agendar snapshots dos volumes após 2 anos** está incorreta, pois RAID (Redundant Array of Independent Disks) é apenas uma tecnologia de virtualização de armazenamento de dados que combina vários dispositivos de armazenamento para obter maior desempenho ou durabilidade dos dados. O RAID 0 pode distribuir vários volumes para obter um desempenho de E/S superior ao de um único volume. Por outro lado, o RAID 1 pode espelhar dois volumes para obter redundância na instância.

Referências:

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>
- <https://docs.aws.amazon.com/efs/latest/ug/lifecycle-management-efs.html>
- https://docs.aws.amazon.com/efs/latest/ug/API_LifecyclePolicy.html
- <https://aws.amazon.com/s3/faqs/>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

50 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Um Arquiteto de Soluções recém-contratado foi designado para gerenciar um conjunto de modelos do CloudFormation usados na arquitetura de nuvem da empresa na AWS. O Arquiteto acessou os modelos e tentou analisar a política de IAM configurada para um bucket do S3.

```
{  
    "Versão": "2012-10-17",  
    "Declaração": [  
        {  
            "Efeito": "Permitir",  
            "Ação": [  
                "s3:Obter*",  
                "s3:Lista*"  
            ],  
            "Recurso": "*"  
        },  
        {  
            "Efeito": "Permitir",  
            "Ação": "s3:PutObject",  
            "Recurso": "arn:aws:s3:::boracay/*"  
        }  
    ]  
}
```

O que a política de IAM acima permite? (Selecione TRÊS.)

Um usuário do IAM com esta política do IAM tem permissão para ler objetos de todos os buckets do S3 de propriedade da conta.

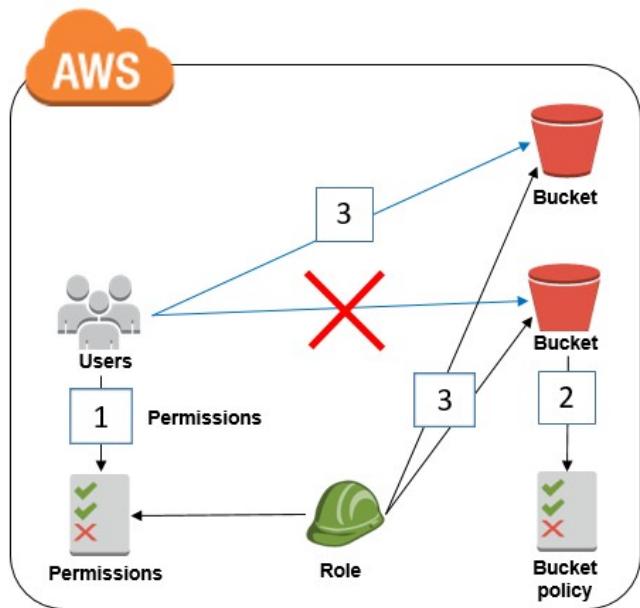
Um usuário do IAM com esta política do IAM tem permissão para gravar objetos no **boracaybucket do S3.**

Um usuário do IAM com esta política do IAM tem permissão para ler objetos do **boracaybucket do S3.**

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

As políticas do IAM definem permissões para ações, independentemente do método usado para executá-las. Por exemplo, se uma política permitir a ação **GetUser**, um usuário com essa política poderá obter informações do usuário no Console de Gerenciamento da AWS, na CLI da AWS ou na API da AWS. Ao criar um usuário do IAM, você pode optar por permitir acesso ao console ou programático. Se o acesso ao console

for permitido, o usuário do IAM poderá fazer login no console usando um nome de usuário e uma senha. Ou, se o acesso programático for permitido, o usuário poderá usar chaves de acesso para trabalhar com a CLI ou a API.



Com base na política do IAM fornecida, o usuário só tem permissão para obter, gravar e listar todos os objetos do **boracay**bucket S3. Isso **s3:PutObject**significa basicamente que você pode enviar uma solicitação de objeto PUT ao bucket S3 para armazenar dados.

Portanto, as respostas corretas são:

- **Um usuário do IAM com esta política do IAM tem permissão para ler objetos de todos os buckets do S3 de propriedade da conta.**

- **Um usuário do IAM com esta política do IAM tem permissão para gravar objetos no **boracay**bucket do S3.**

A opção que diz: **Um usuário do IAM com esta política do IAM tem permissão para alterar os direitos de acesso para o **boracay**bucket do S3** está incorreta porque o modelo não tem nenhuma instrução que permita ao usuário alterar os direitos de acesso no bucket.

A opção que diz: **Um usuário do IAM com esta política do IAM tem permissão para ler objetos no **boracay**bucket do S3, mas não tem permissão para listar os objetos no bucket** está incorreta porque pode ser visto claramente no modelo que há um **s3>List***que permite ao usuário listar objetos.

A opção que diz: **Um usuário do IAM com esta política do IAM tem permissão para ler e excluir objetos do **boracay**bucket do S3** está incorreta. Embora você possa ler objetos do bucket, não pode excluir nenhum objeto.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectOps.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

51. PERGUNTA

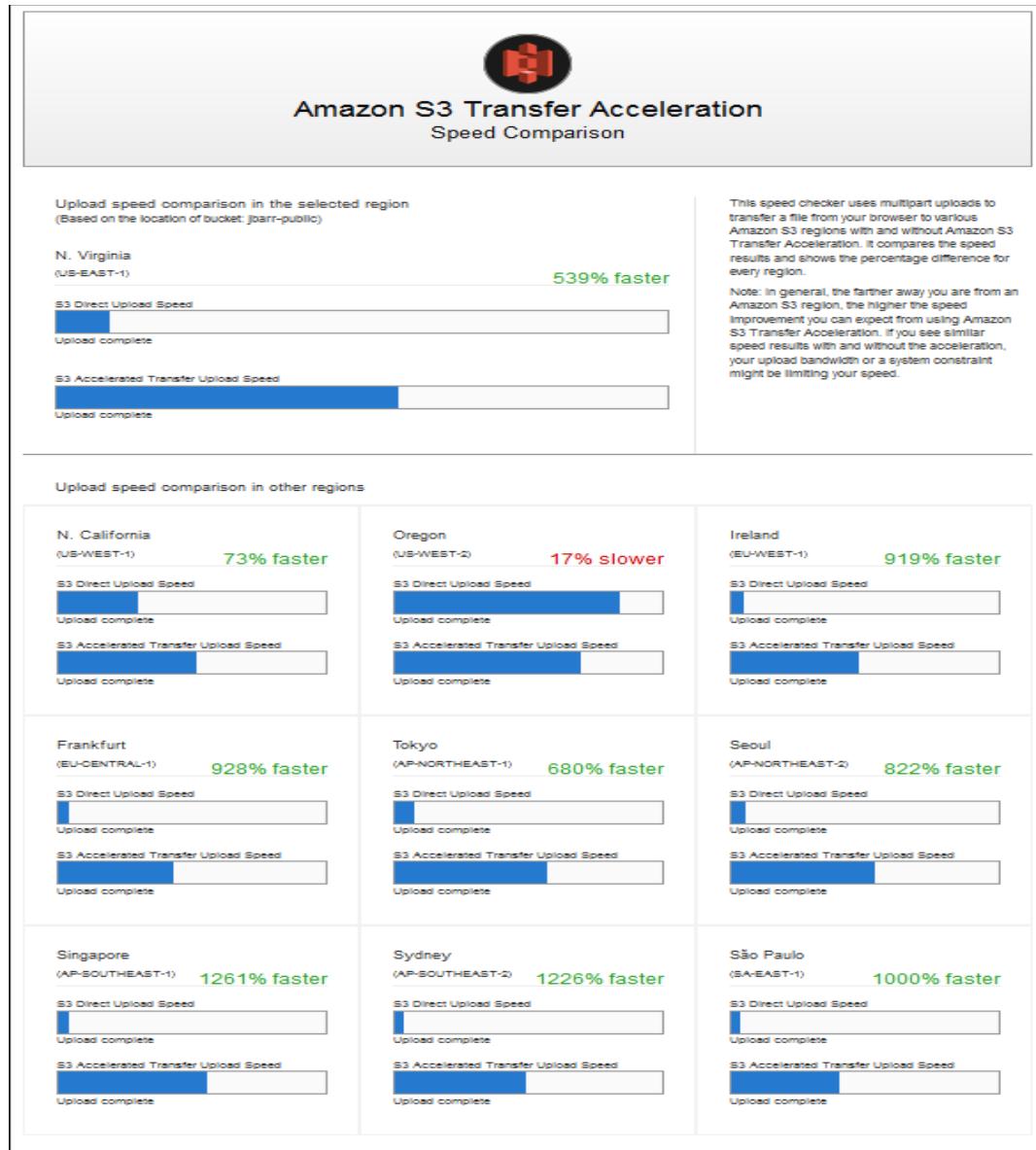
Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa coleta dados atmosféricos, como temperatura, pressão atmosférica e umidade, de diferentes países. Cada local está equipado com diversos instrumentos meteorológicos e uma conexão de internet de alta velocidade. A média de dados coletados em cada local é de cerca de 500 GB e será analisada por um

aplicativo de previsão do tempo hospedado no norte da Virgínia. O Arquiteto de Soluções deve determinar a maneira mais rápida de agregar todos os dados. Qual das seguintes opções pode satisfazer o requisito fornecido?

Habilite a Aceleração de Transferência no bucket de destino e carregue os dados coletados usando o Multipart Upload.

O Amazon S3 é um serviço de armazenamento de objetos criado para armazenar e recuperar qualquer quantidade de dados de qualquer lugar na internet. É um serviço de armazenamento simples que oferece durabilidade, disponibilidade, desempenho, segurança e escalabilidade praticamente ilimitada, líderes do setor, a custos baixíssimos. O Amazon S3 também foi projetado para ser altamente flexível. Armazene qualquer tipo e quantidade de dados que desejar; leia o mesmo dado um milhão de vezes ou apenas para recuperação de desastres emergenciais; crie um aplicativo FTP simples ou um aplicativo web sofisticado.



Como o aplicativo de previsão do tempo está localizado na Virgínia do Norte, você precisa transferir todos os dados na mesma região da AWS. Com o Amazon S3 Transfer Acceleration, você pode acelerar as transferências de conteúdo de e para o Amazon S3 em até 50% a 500% para transferências de longa distância de objetos maiores. O upload multipartes permite que você carregue um único objeto como um conjunto de partes. Após o upload de todas as partes do seu objeto, o Amazon S3 apresenta os dados como um único objeto. Essa abordagem é a maneira mais rápida de agregar todos os dados.

Portanto, a resposta correta é: **Habilite a Aceleração de Transferência no bucket de destino e carregue os dados coletados usando o Multipart Upload.**

A opção que diz: **Carregar os dados para o bucket do Amazon S3 mais próximo. Configurar uma replicação entre regiões e copiar os objetos para o bucket de destino** está incorreta, pois a replicação dos objetos para o bucket de destino normalmente leva cerca de 15 minutos. Observe que o requisito neste cenário é agregar os dados da maneira mais rápida possível.

A opção que diz: **Usar o AWS Snowball Edge para transferir grandes quantidades de dados** está incorreta porque o tempo de ponta a ponta para transferir até 80 TB de dados para o AWS Snowball Edge é de aproximadamente apenas uma semana.

A opção que diz: **Configurar uma conexão VPN Site-to-Site** está incorreta porque a configuração de uma conexão VPN não é necessária neste cenário. A VPN Site-to-Site é usada apenas para estabelecer conexões seguras entre uma rede local e a Amazon VPC. Além disso, essa abordagem não é a maneira mais rápida de transferir seus dados. Você deve usar o Amazon S3 Transfer Acceleration.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

52 . PERGUNTA

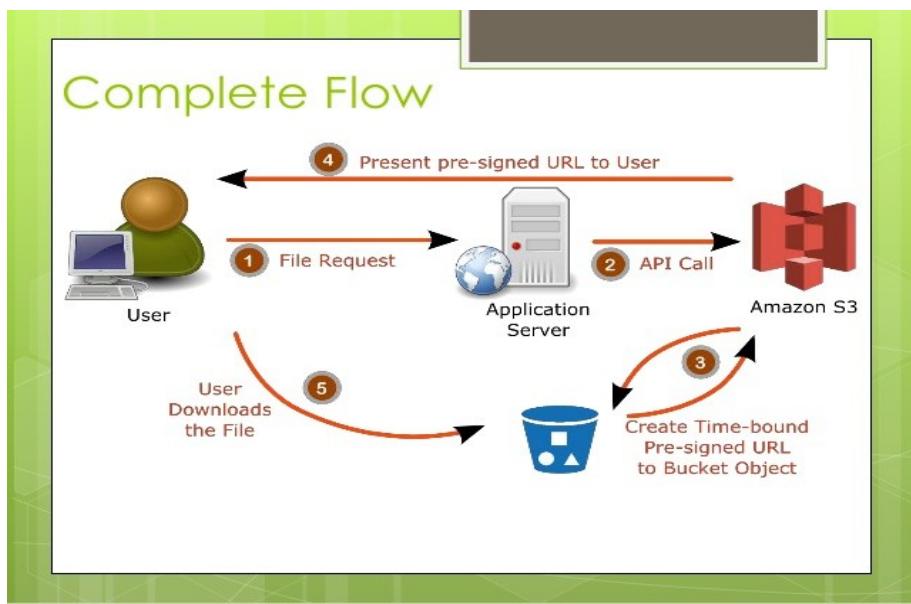
Categoria: CSAA – Design de Arquiteturas Seguras

Um site de compartilhamento de fotos de viagens está usando o Amazon S3 para fornecer fotos de alta qualidade aos visitantes. Após alguns dias, descobriu-se que outros sites de viagens estavam criando links para essas fotos e as utilizando. Isso resultou em perdas financeiras para a empresa. Qual é o método MAIS eficaz para mitigar esse problema?

Configure seu bucket S3 para remover o acesso público de leitura e usar URLs pré-assinadas com datas de expiração.

No Amazon S3, todos os objetos são privados por padrão. Somente o proprietário do objeto tem permissão para acessá-los. No entanto, o proprietário do objeto pode, opcionalmente, compartilhá-los com outras pessoas criando uma URL pré-assinada, usando suas próprias credenciais de segurança, para conceder permissão por tempo limitado para baixar os objetos.

Ao criar uma URL pré-assinada para seu objeto, você deve fornecer suas credenciais de segurança, especificar um nome de bucket, uma chave de objeto, especificar o método HTTP (GET para baixar o objeto) e a data e hora de expiração. As URLs pré-assinadas são válidas apenas pelo período especificado.



Qualquer pessoa que receber a URL pré-assinada poderá acessar o objeto. Por exemplo, se você tiver um vídeo no seu bucket e tanto o bucket quanto o objeto forem privados, você poderá compartilhar o vídeo com outras pessoas gerando uma URL pré-assinada.

Portanto, a resposta correta é: **configure seu bucket S3 para remover o acesso público de leitura e usar URLs pré-assinadas com datas de expiração.**

A opção que diz: **Usar distribuições do Amazon CloudFront para suas fotos** está incorreta. O CloudFront é principalmente um serviço de rede de distribuição de conteúdo que acelera a entrega de conteúdo aos seus clientes.

A opção que diz: **Bloquear os endereços IP dos sites ofensivos usando NACL** também está incorreta. Bloquear endereços IP usando NACLS não é um método muito eficiente, pois uma mudança rápida no endereço IP contornaria facilmente essa configuração.

A opção que diz: **Armazenar e disponibilizar privadamente as fotos de alta qualidade no Amazon WorkDocs** está incorreta, pois o WorkDocs é simplesmente um serviço de criação, armazenamento e colaboração de conteúdo totalmente gerenciado e seguro. Não é um serviço adequado para armazenar conteúdo estático. O Amazon WorkDocs é mais frequentemente usado para criar, editar e compartilhar documentos facilmente para colaboração, e não para disponibilizar dados de objetos como o Amazon S3.

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectOperations.html>

Confira esta folha de dicas do Amazon CloudFront:

<https://tutorialsdojo.com/amazon-cloudfront/>

Comparação de folhas de dicas de serviços da AWS:

<https://tutorialsdojo.com/comparison-of-aws-services/>

53 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

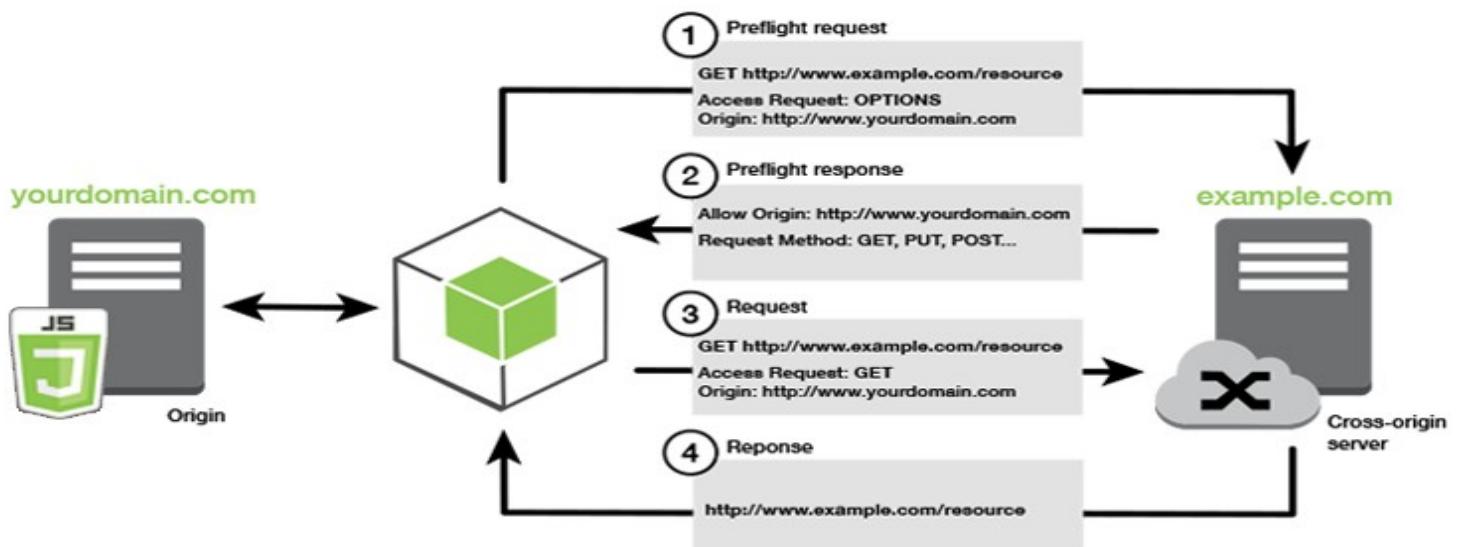
Um Arquiteto de Soluções está hospedando um site em um bucket do Amazon S3 chamado `tutorialsdojo`. Os usuários carregam o site usando a seguinte URL: `http://tutorialsdojo.s3-website-us-east-1.amazonaws.com`. Um novo requisito foi introduzido para adicionar JavaScript nas páginas da web para

fazer `GET` solicitações HTTP autenticadas no mesmo bucket usando o endpoint da API do S3 (`tutorialsdojo.s3.amazonaws.com`). No entanto, durante os testes, o navegador da web bloqueia o JavaScript, impedindo que essas solicitações sejam permitidas.

Qual das seguintes opções é a solução MAIS adequada para implementar neste cenário?

Habilite a configuração de compartilhamento de recursos entre origens (CORS) no bucket.

O compartilhamento de recursos entre origens (CORS) define uma maneira para que aplicativos web clientes carregados em um domínio interajam com recursos de outro domínio. Com o suporte ao CORS, você pode criar aplicativos web avançados do lado do cliente com o Amazon S3 e permitir seletivamente o acesso entre origens aos seus recursos do Amazon S3.



Suponha que você esteja hospedando um site em um bucket do Amazon S3 chamado `your-website` e seus usuários carreguem o endpoint do site `http://your-website.s3-website-us-east-1.amazonaws.com`. Agora, você deseja usar JavaScript nas páginas da web armazenadas neste bucket para poder fazer solicitações GET e PUT autenticadas no mesmo bucket usando o endpoint da API do Amazon S3 para o bucket, `your-website.s3.amazonaws.com`. Um navegador normalmente bloquearia o JavaScript de permitir essas solicitações, mas com o CORS você pode configurar seu bucket para habilitar explicitamente solicitações entre origens de `your-website.s3-website-us-east-1.amazonaws.com`.

Portanto, a resposta correta é: **Habilitar a configuração de compartilhamento de recursos entre origens (CORS) no bucket.**

A opção que diz: **Habilitar acesso entre contas** está incorreta porque o acesso entre contas é apenas um recurso no IAM e não no Amazon S3.

A opção que diz: **Habilitar balanceamento de carga entre zonas** está incorreta porque o balanceamento de carga entre zonas é usado somente no ELB e não no S3.

A opção que diz: **Habilitar replicação entre regiões (CRR)** está incorreta porque CRR é uma configuração em nível de bucket que permite a cópia automática e assíncrona de objetos entre buckets em diferentes regiões da AWS.

Referências:

<http://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ManageCorsUsing.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

Categoria: CSAA - Design de Arquiteturas de Alto Desempenho

Uma rede social popular está hospedada na AWS e usa uma tabela do Amazon DynamoDB como banco de dados. É necessário implementar um recurso de "seguir", que permite aos usuários assinar determinadas atualizações feitas por um usuário específico e receber notificações por e-mail. Qual das seguintes opções é a solução mais adequada para implementar para atender ao requisito?

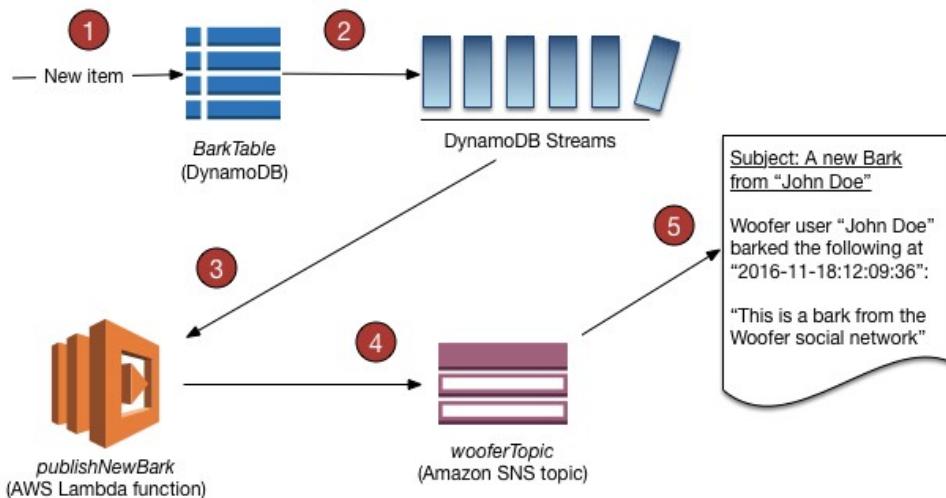
Habilite o DynamoDB Stream e crie um gatilho do AWS Lambda, bem como a função do IAM que contém todas as permissões que a função do Lambda precisará em tempo de execução. Os dados do registro do stream serão processados pela função do Lambda, que publicará uma mensagem no tópico do Amazon SNS, notificando os assinantes por e-mail.

Um **fluxo do DynamoDB** é um fluxo ordenado de informações sobre alterações em itens em uma tabela do Amazon DynamoDB. Quando você habilita um fluxo em uma tabela, o DynamoDB captura informações sobre cada modificação nos itens de dados da tabela.

Sempre que um aplicativo cria, atualiza ou exclui itens na tabela, o DynamoDB Streams grava um registro de fluxo com os atributos de chave primária dos itens modificados. Um registro de fluxo contém informações sobre uma modificação de dados em um único item em uma tabela do DynamoDB. Você pode configurar o fluxo para que os registros de fluxo capturem informações adicionais, como as imagens "antes" e "depois" dos itens modificados.

O Amazon DynamoDB é integrado ao AWS Lambda para que você possa criar gatilhos – trechos de código que respondem automaticamente a eventos nos Streams do DynamoDB. Com gatilhos, você pode criar aplicativos que reagem a modificações de dados em tabelas do DynamoDB.

Se você habilitar o DynamoDB Streams em uma tabela, poderá associar o ARN do fluxo a uma função do Lambda que você escrever. Imediatamente após a modificação de um item na tabela, um novo registro aparecerá no fluxo da tabela. O AWS Lambda consulta o fluxo e invoca sua função do Lambda de forma síncrona ao detectar novos registros de fluxo. A função do Lambda pode executar qualquer ação que você especificar, como enviar uma notificação ou iniciar um fluxo de trabalho.



Portanto, a resposta correta é: **habilite o DynamoDB Stream e crie um gatilho do AWS Lambda, bem como a função do IAM que contém todas as permissões que a função Lambda precisará em tempo de execução. Os dados do registro do stream serão processados pela função Lambda, que então publicará uma mensagem no tópico do Amazon SNS, notificando os assinantes por e-mail .**

A opção que diz: **Usando a Biblioteca de Cliente do Amazon Kinesis (KCL), escreva um aplicativo que utilize o Adaptador Kinesis do DynamoDB Streams para buscar dados do endpoint do DynamoDB Streams. Quando houver atualizações feitas por um usuário específico, notificar os assinantes por e-mail usando o Amazon SNS** está incorreta. Embora esta seja uma solução válida, falta uma etapa vital, que é habilitar o DynamoDB Streams. Com o Adaptador Kinesis do DynamoDB Streams instalado, você pode começar

a desenvolver aplicativos por meio da interface KCL, com as chamadas de API direcionadas diretamente ao endpoint do DynamoDB Streams. Lembre-se de que o recurso DynamoDB Stream não está habilitado por padrão.

A opção que diz: **Criar uma função do AWS Lambda que use o adaptador Amazon Kinesis do DynamoDB Streams, que buscará dados do endpoint do DynamoDB Streams. Configurar um tópico do Amazon SNS que notificará os assinantes por e-mail quando houver uma atualização feita por um usuário específico** está incorreta porque, assim como no exemplo acima, você precisa habilitar manualmente o DynamoDB Streams antes de poder usar seu endpoint.

A opção que diz: **Configurar um cluster DAX para acessar a tabela de origem do DynamoDB. Criar um novo gatilho do DynamoDB e uma função do AWS Lambda. Para cada atualização feita nos dados do usuário, o gatilho enviará dados para a função do Lambda, que notificará os assinantes por e-mail usando o Amazon SNS. Configurar um cluster DAX para acessar a tabela de origem do DynamoDB. Criar um novo gatilho do DynamoDB e uma função do Lambda. Para cada atualização feita nos dados do usuário, o gatilho enviará dados para a função do Lambda, que notificará os assinantes por e-mail usando o SNS** está incorreta porque o recurso DynamoDB Accelerator (DAX) é usado principalmente para melhorar significativamente o desempenho de leitura na memória do seu banco de dados, e não para capturar a sequência ordenada por tempo das modificações no nível do item. Você deve usar o DynamoDB Streams neste cenário.

Referências:

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.Tutorial.html>

Confira esta folha de dicas do Amazon DynamoDB:

<https://tutorialsdojo.com/amazon-dynamodb/>

55 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

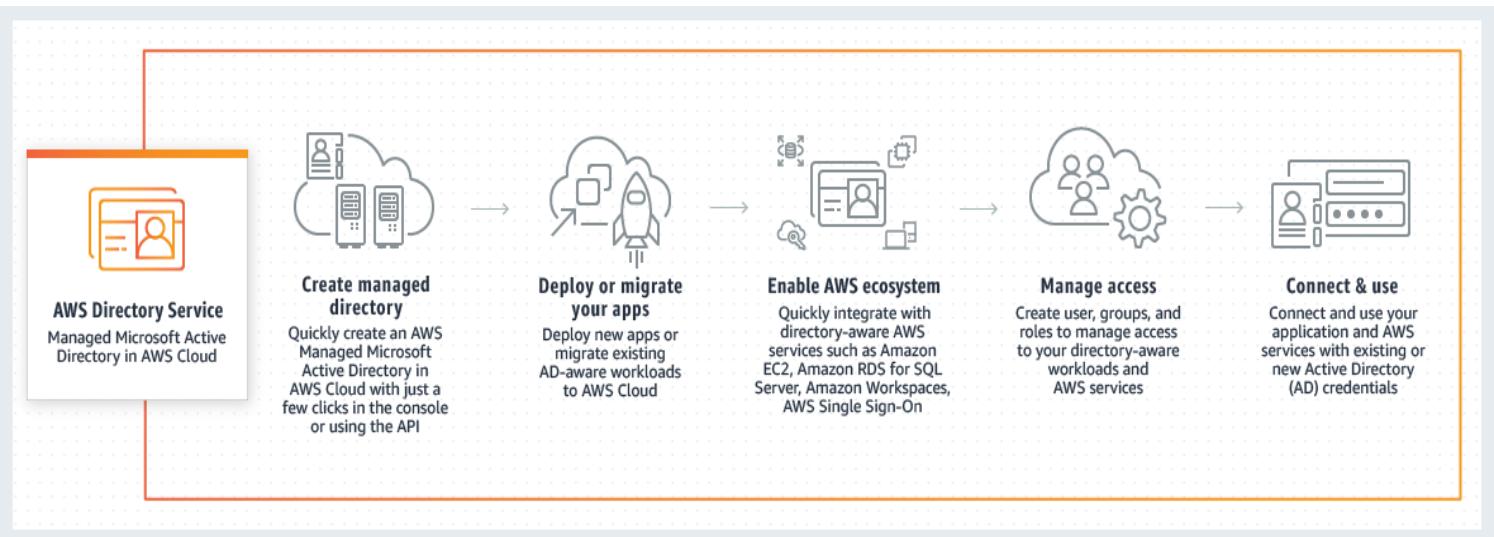
Uma empresa de telecomunicações está planejando conceder acesso ao Console da AWS aos seus desenvolvedores. A política da empresa exige o uso de federação de identidades e controle de acesso baseado em funções. Atualmente, as funções já são atribuídas por meio de grupos no Active Directory corporativo.

Neste cenário, qual combinação dos seguintes serviços pode fornecer aos desenvolvedores acesso ao console da AWS? (Selecione DUAS.)

Conektor AD do Serviço de Diretório AWS

Funções do IAM

O AWS Directory Service oferece diversas maneiras de usar o Amazon Cloud Directory e o Microsoft Active Directory (AD) com outros serviços da AWS. Os diretórios armazenam informações sobre usuários, grupos e dispositivos, e os administradores os utilizam para gerenciar o acesso a informações e recursos. O AWS Directory Service oferece diversas opções de diretório para clientes que desejam usar aplicativos compatíveis com o Microsoft AD ou o Lightweight Directory Access Protocol (LDAP) na nuvem. Ele também oferece essas mesmas opções para desenvolvedores que precisam de um diretório para gerenciar usuários, grupos, dispositivos e acesso.



Considerando que a empresa utiliza um Active Directory corporativo, é melhor utilizar o Conector AD do AWS Directory Service para facilitar a integração. Além disso, como as funções já são atribuídas por meio de grupos no Active Directory corporativo, seria melhor utilizar também as Funções do IAM. Observe que você pode atribuir uma Função do IAM aos usuários ou grupos do seu Active Directory após a integração com a sua VPC por meio do Conector AD do AWS Directory Service.

Portanto, as respostas corretas são:

- **Conector AD do Serviço de Diretório AWS.**
- **Funções do IAM.**

O **AWS Directory Service Simple AD** está , pois fornece apenas um subconjunto dos recursos oferecidos pelo AWS Managed Microsoft AD, incluindo a capacidade de gerenciar contas de usuários e associações de grupos, criar e aplicar políticas de grupo, conectar-se com segurança a instâncias do Amazon EC2 e fornecer logon único (SSO) baseado em Kerberos. Nesse cenário, o componente mais adequado é o AD Connector, pois é um gateway de diretório com o qual você pode redirecionar solicitações de diretório para o Microsoft Active Directory local.

A opção "**Grupos do IAM**" está incorreta, pois se trata apenas de uma coleção de usuários do IAM . Os grupos permitem especificar permissões para vários usuários, o que pode facilitar o gerenciamento das permissões desses usuários. Nesse cenário, a opção mais adequada é usar "Funções do IAM" para obter permissões para criar recursos do AWS Directory Service.

AWS Lambda está porque é usado principalmente para computação sem servidor.

Referências:

<https://aws.amazon.com/blogs/security/como-conectar-seu-diretório-ativo-local-ao-aws-usando-conector-de-anúncios/>

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_getting_started.html

Confira estas folhas de dicas do AWS IAM e do Directory Service:

<https://tutorialsdojo.com/aws-identity-and-access-management-iam/>

<https://tutorialsdojo.com/aws-directory-service/>

Aqui está um tutorial em vídeo sobre o AWS Directory Service:

<https://youtu.be/4XeqotTYBtY>

56. PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

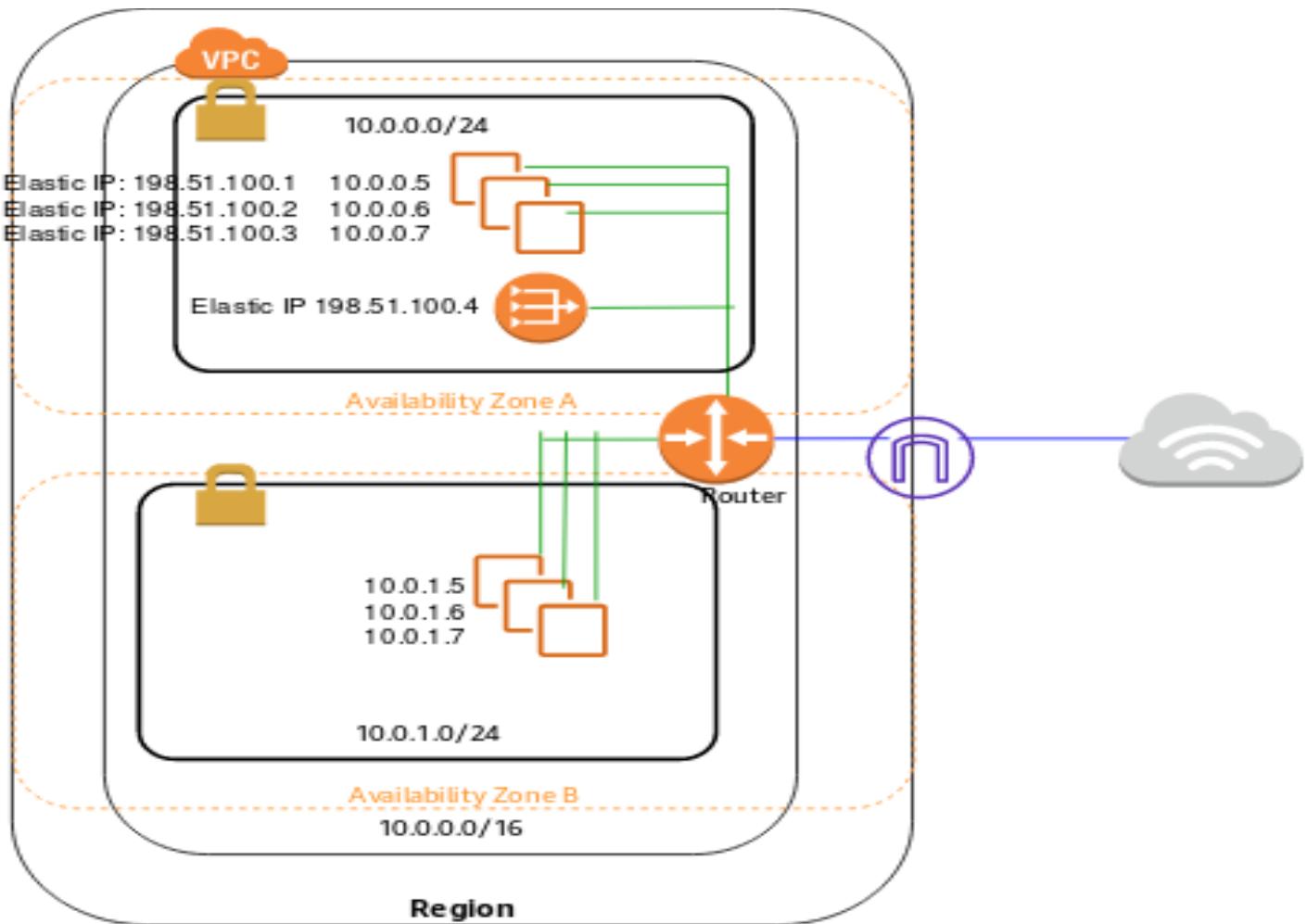
Uma aplicação consiste em várias instâncias do Amazon EC2 em sub-redes privadas em diferentes zonas de disponibilidade. A aplicação utiliza um único Gateway NAT para baixar patches de software da internet para as instâncias. É necessário proteger a aplicação de um único ponto de falha quando o Gateway NAT encontra uma falha ou se sua zona de disponibilidade fica inativa.

Como o arquiteto de soluções deve redesenhar a arquitetura para que ela seja mais disponível e econômica?

Crie um Gateway NAT em cada zona de disponibilidade. Configure a tabela de rotas em cada sub-rede privada para garantir que as instâncias usem o Gateway NAT na mesma zona de disponibilidade.

Um **Gateway NAT** é um serviço de Tradução de Endereços de Rede (NAT) gerenciado e altamente disponível para seus recursos em uma sub-rede privada acessarem a Internet. O gateway NAT é criado em uma Zona de Disponibilidade específica e implementado com redundância nessa zona.

Você deve criar um gateway NAT em uma sub-rede pública para permitir que instâncias em uma sub-rede privada se conectem à Internet ou a outros serviços da AWS, mas impedir que a Internet inicie uma conexão com essas instâncias.



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

Portanto, a resposta correta é: **Crie um Gateway NAT em cada zona de disponibilidade. Configure a tabela de rotas em cada sub-rede privada para garantir que as instâncias usem o Gateway NAT na mesma zona de disponibilidade**.

A opção que diz: **Criar um Gateway NAT em cada zona de disponibilidade. Configurar a tabela de rotas em cada sub-rede pública para garantir que as instâncias usem o Gateway NAT na mesma zona de disponibilidade** está incorreta, pois você deve configurar a tabela de rotas na sub-rede privada e não na pública para associar as instâncias corretas na sub-rede privada.

As opções que dizem: **Criar dois Gateways NAT em cada zona de disponibilidade. Configurar a tabela de rotas em cada sub-rede pública para garantir que as instâncias usem o Gateway NAT na mesma zona de disponibilidade** estão incorretas, pois você precisa configurar o Gateway NAT principalmente na sub-rede privada para permitir o acesso de saída à Internet para instâncias privadas.

As opções que dizem: **Criar três Gateways NAT em cada zona de disponibilidade. Configurar a tabela de rotas em cada sub-rede privada para garantir que as instâncias usem o Gateway NAT na mesma zona de disponibilidade** estão incorretas, pois a única necessidade aqui é garantir o tráfego de saída para instâncias privadas, e adicionar vários Gateways NAT não se alinha com a otimização de custos, a menos que seja explicitamente necessário para alta disponibilidade.

Referências:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

Confira esta folha de dicas do Amazon VPC:

<https://tutorialsdojo.com/amazon-vpc/>

57 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

Uma plataforma de compras online é hospedada em um grupo de Auto Scaling de instâncias Spot do Amazon EC2 e utiliza o Amazon Aurora PostgreSQL como banco de dados. Ela é necessária para otimizar as cargas de trabalho do banco de dados no cluster, direcionando o tráfego de produção para instâncias de alta capacidade e encaminhando as consultas de relatórios da equipe interna para as instâncias de baixa capacidade.

Qual é a configuração mais adequada para que o aplicativo e o cluster de banco de dados Aurora atendam a esse requisito?

Crie um ponto de extremidade personalizado no Aurora com base nos critérios especificados para o tráfego de produção e outro ponto de extremidade personalizado para lidar com as consultas de relatórios.

O Amazon Aurora normalmente envolve um cluster de instâncias de banco de dados em vez de uma única instância. Cada conexão é gerenciada por uma instância de banco de dados específica. Quando você se conecta a um cluster do Aurora, o nome do host e a porta especificados apontam para um manipulador intermediário chamado endpoint. O Aurora usa o mecanismo de endpoint para abstrair essas conexões. Assim, você não precisa codificar todos os nomes de host ou escrever sua própria lógica para balanceamento de carga e redirecionamento de conexões quando algumas instâncias de banco de dados não estiverem disponíveis.

Para determinadas tarefas do Aurora, diferentes instâncias ou grupos de instâncias desempenham funções distintas. Por exemplo, a instância primária lida com todas as instruções da linguagem de definição de dados (DDL) e da linguagem de manipulação de dados (DML). Até 15 réplicas do Aurora lidam com tráfego de consulta somente leitura.

DB identifier	Role	Engine	Class	Status	CPU	Current
tutorialsdojo-1	Cluster	Aurora MySQL	-	Available		
tutorialsdojo	Writer	Aurora MySQL	db.t2.small	Available	9.33%	
tutorialsdojo-ap-southeast-2b	Reader	Aurora MySQL	db.t2.small	Available	7.70%	

- [Connectivity & security](#)
- [Monitoring](#)
- [Logs & events](#)
- [Configuration](#)
- [Maintenance & backups](#)
- [Tags](#)

Endpoints (2)	Edit	Delete	Create custom endpoint	
<input type="text"/> Filter endpoint	<	1	>	Reset
Endpoint name	Status	Type	Port	
tutorialsdojo-1.cluster-ro-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com	Available	Reader	3306	
tutorialsdojo-1.cluster-cerpn6ov4bsw.ap-southeast-2.rds.amazonaws.com	Available	Writer	3306	

Usando endpoints, você pode mapear cada conexão para a instância ou grupo de instâncias apropriado, com base no seu caso de uso. Por exemplo, para executar instruções DDL, você pode se conectar à instância primária. Para executar consultas, você pode se conectar ao endpoint do leitor, com o Aurora realizando automaticamente o balanceamento de carga entre todas as réplicas do Aurora. Para clusters com instâncias de banco de dados de diferentes capacidades ou configurações, você pode se conectar a endpoints personalizados associados a diferentes subconjuntos de instâncias de banco de dados. Para diagnóstico ou ajuste, você pode se conectar a um endpoint de instância específico para examinar detalhes sobre uma instância de banco de dados específica.

O endpoint personalizado fornece conexões de banco de dados com balanceamento de carga com base em critérios diferentes da capacidade somente leitura ou leitura/gravação das instâncias de banco de dados. Por exemplo, você pode definir um endpoint personalizado para se conectar a instâncias que usam uma classe de instância específica da AWS ou um grupo de parâmetros de banco de dados específico. Em seguida, você pode informar grupos específicos de usuários sobre esse endpoint personalizado. Por exemplo, você pode direcionar usuários internos para instâncias de baixa capacidade para geração de relatórios ou consultas ad hoc (únicas), e direcionar o tráfego de produção para instâncias de alta capacidade.

Portanto, a resposta correta é: **Crie um ponto de extremidade personalizado no Aurora com base nos critérios especificados para o tráfego de produção e outro ponto de extremidade personalizado para lidar com as consultas de relatórios.**

A opção que diz: **Configurar seu aplicativo para usar o endpoint do leitor para o tráfego de produção e consultas de relatórios, o que permitirá que seu banco de dados Aurora execute automaticamente o balanceamento de carga entre todas as réplicas do Aurora,** está incorreta. Embora seja verdade que um endpoint do leitor permite que seu banco de dados Aurora execute automaticamente o balanceamento de carga entre todas as réplicas do Aurora, ele é bastante limitado a realizar apenas operações de leitura. Você ainda precisa usar um endpoint personalizado para balancear a carga das conexões do banco de dados com base nos critérios especificados.

A opção que diz: **Em seu aplicativo, use o endpoint da instância do seu banco de dados Aurora para manipular o tráfego de produção de entrada e use o endpoint do cluster para manipular consultas de**

relatórios está incorreta porque um endpoint do cluster (também conhecido como endpoint de gravação) para um cluster de banco de dados Aurora simplesmente se conecta à instância de banco de dados primária atual para esse cluster de banco de dados. Esse endpoint pode executar operações de gravação no banco de dados, como instruções DDL, o que é perfeito para manipular o tráfego de produção, mas não é adequado para manipular consultas para relatórios, pois não haverá operações de gravação no banco de dados a serem enviadas. Além disso, o endpoint não aponta para instâncias de baixa ou alta capacidade, conforme o requisito. Uma solução melhor para isso é usar um endpoint personalizado.

A opção que diz: **Não fazer nada, pois, por padrão, o Aurora direcionará automaticamente o tráfego de produção para suas instâncias de alta capacidade e as consultas de relatórios para suas instâncias de baixa capacidade** está incorreta, pois o Aurora não faz isso por padrão. Você precisa criar endpoints personalizados para atender a esse requisito.

Referências:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.Endpoints.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Endpoints.Custom.html>

Confira esta folha de dicas do Amazon Aurora:

<https://tutorialsdojo.com/amazon-aurora/>

58 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

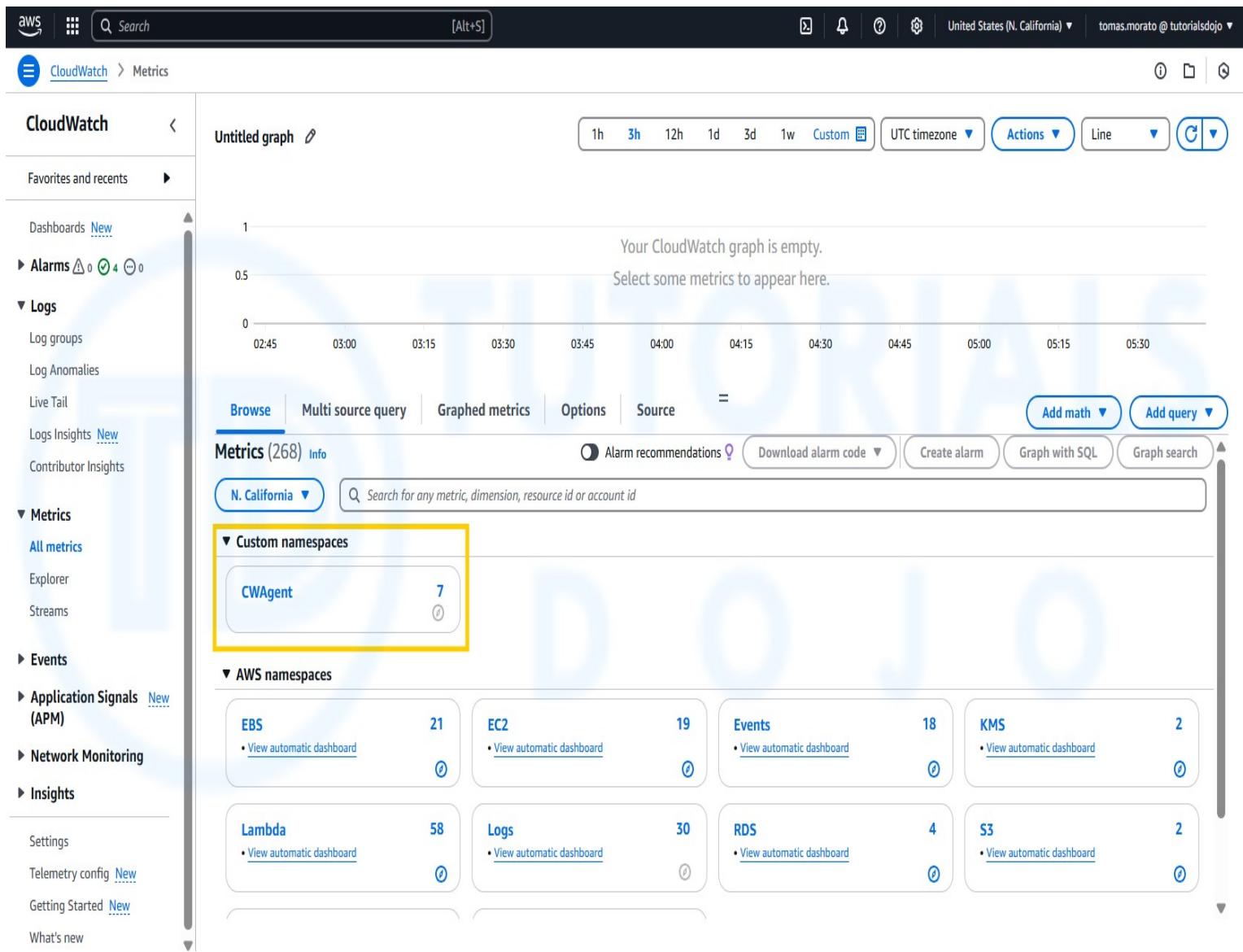
Uma empresa possui uma arquitetura de nuvem composta por instâncias Linux e Windows do Amazon EC2 que processam altos volumes de dados financeiros 24 horas por dia, 7 dias por semana. Para garantir alta disponibilidade dos sistemas, o Arquiteto de Soluções deve criar uma solução que permita o monitoramento das métricas de utilização de memória e disco para todas as instâncias.

Qual das seguintes opções é a solução de monitoramento mais adequada para implementar?

Instale o agente do Amazon CloudWatch em todas as instâncias do EC2 que coletam dados de utilização de memória e disco. Visualize as métricas personalizadas no console do CloudWatch.

O Amazon CloudWatch disponibiliza métricas do Amazon EC2 para você monitorar a utilização da CPU, a utilização da rede, o desempenho do disco e as leituras/gravações em disco. Caso precise monitorar os itens abaixo, prepare uma métrica personalizada usando um script Perl ou outro shell, pois não há métricas prontas para uso para os seguintes itens:

- Utilização de memória
- Utilização de troca de disco
- Utilização do espaço em disco
- Utilização do arquivo de paginação
- Coleta de logs



Observe que há um agente CloudWatch multiplataforma que pode ser instalado em instâncias Linux e Windows. Você pode usar um único agente para coletar métricas do sistema e arquivos de log de instâncias do Amazon EC2 e servidores locais. Este agente é compatível com Windows Server e Linux e permite selecionar as métricas a serem coletadas, incluindo métricas de sub-recursos, como núcleo por CPU. Recomenda-se usar o novo agente em vez dos scripts de monitoramento antigos para coletar métricas e logs.

Portanto, a resposta correta é: **instalar o agente do Amazon CloudWatch em todas as instâncias do EC2 que coletam dados de utilização de memória e disco. Visualizar as métricas personalizadas no console do CloudWatch.**

A opção que diz: **Usar a configuração padrão do Amazon CloudWatch para instâncias do EC2 onde as métricas de utilização de memória e disco já estão disponíveis. Instalar o Agente do AWS Systems Manager (SSM) em todas as instâncias do EC2** está incorreta porque, por padrão, o CloudWatch não fornece automaticamente as métricas de utilização de memória e disco das suas instâncias. Você precisa simplesmente configurar métricas personalizadas do CloudWatch para monitorar a memória, a troca de disco, o espaço em disco e a utilização do arquivo de paginação das suas instâncias.

A opção que diz: **Habilite a opção Monitoramento Avançado no EC2 e instale o agente do Amazon CloudWatch em todas as instâncias do EC2 para poder visualizar a utilização de memória e disco no painel do CloudWatch** está incorreta, pois o Monitoramento Avançado é um recurso exclusivo do Amazon RDS. Por padrão, as métricas do Monitoramento Avançado são armazenadas por apenas 30 dias nos logs do CloudWatch.

A opção que diz: **Usar o Amazon Inspector e instalar o agente do Inspector em todas as instâncias do EC2** está incorreta porque o Amazon Inspector é principalmente um serviço automatizado de avaliação de

segurança que ajuda a testar a acessibilidade de rede das suas instâncias do Amazon EC2 e o estado de segurança dos seus aplicativos em execução nessas instâncias. Ele não fornece uma métrica personalizada para rastrear a utilização de memória e disco de cada instância do EC2 na sua VPC.

Referências:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html#using_put_script

Confira esta folha de dicas do Amazon CloudWatch:

<https://tutorialsdojo.com/amazon-cloudwatch/>

Agente CloudWatch vs Agente SSM vs Scripts de Daemon Personalizados:

<https://tutorialsdojo.com/cloudwatch-agent-vs-ssm-agent-vs-custom-daemon-scripts/>

Comparação de folhas de dicas de serviços da AWS:

<https://tutorialsdojo.com/comparison-of-aws-services/>

59 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Resilientes

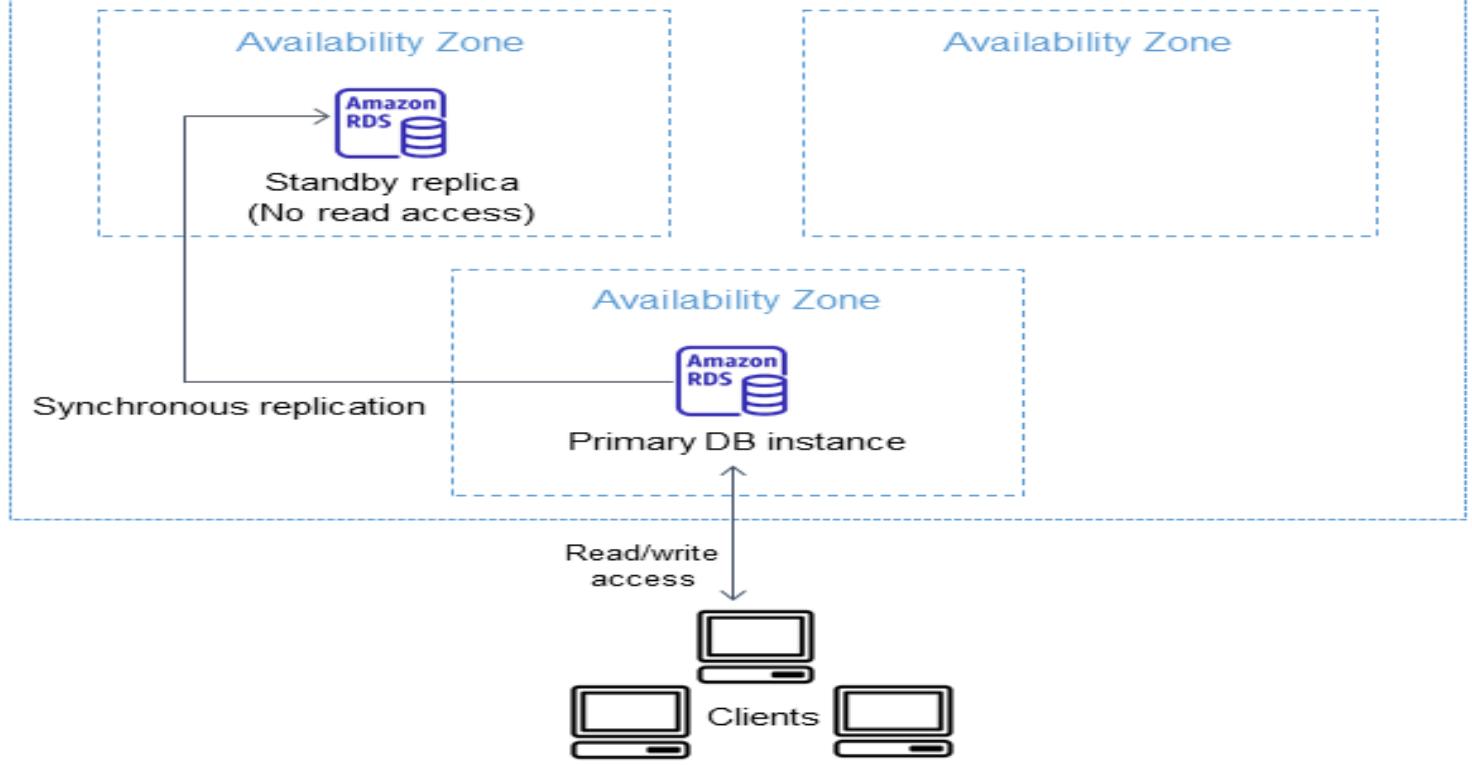
Uma plataforma de negociação Forex, que processa e armazena dados financeiros globais a cada minuto, está hospedada em um data center local e utiliza um banco de dados Oracle. Devido a um recente problema de resfriamento em seu data center, a empresa precisa migrar urgentemente sua infraestrutura para a AWS para melhorar o desempenho de seus aplicativos. Como Arquiteto de Soluções, a responsabilidade é garantir que o banco de dados seja migrado corretamente e permaneça disponível em caso de falha do servidor de banco de dados no futuro.

Qual combinação de ações atenderia ao requisito? (Selecione DUAS.)

Crie um banco de dados Oracle no Amazon RDS com implantações Multi-AZ.

Migrar o banco de dados Oracle para a AWS usando o AWS Database Migration Service

As implantações Multi-AZ do Amazon RDS oferecem disponibilidade e durabilidade aprimoradas para Instâncias de Banco de Dados (BD), tornando-as ideais para cargas de trabalho de bancos de dados de produção. Ao provisionar uma Instância de Banco de Dados Multi-AZ, o Amazon RDS cria automaticamente uma Instância de Banco de Dados primária e replica os dados de forma síncrona para uma instância em espera em uma Zona de Disponibilidade (AZ) diferente. Cada AZ é executada em sua própria infraestrutura fisicamente distinta e independente, e foi projetada para ser altamente confiável.



Em caso de falha de infraestrutura, o Amazon RDS executa um failover automático para o standby (ou para uma réplica de leitura no caso do Amazon Aurora) para que você possa retomar as operações do banco de dados assim que o failover for concluído. Como o endpoint da sua instância de banco de dados permanece o mesmo após um failover, seu aplicativo pode retomar a operação do banco de dados sem a necessidade de intervenção administrativa manual.

Nesse cenário, a melhor configuração do RDS a ser usada é um banco de dados Oracle no RDS com implantações Multi-AZ para garantir alta disponibilidade mesmo se a instância principal do banco de dados cair. Você pode usar o AWS DMS para migrar o banco de dados local para a AWS com tempo de inatividade mínimo e zero perda de dados. Ele suporta mais de 20 mecanismos, incluindo Oracle para Aurora MySQL, MySQL para RDS para MySQL, SQL Server para Aurora PostgreSQL, MongoDB para DocumentDB, Oracle para Redshift e S3.

Portanto, as respostas corretas são:

- **Crie um banco de dados Oracle no Amazon RDS com implantações Multi-AZ.**
- **Migre o banco de dados Oracle para a AWS usando o AWS Database Migration Service.**

A opção que diz: **Iniciar uma instância de banco de dados Oracle no Amazon RDS com o Recovery Manager (RMAN) habilitado** está incorreta porque o Oracle RMAN não é suportado no RDS.

A opção que diz: **Converter o esquema do banco de dados usando a Ferramenta de Conversão de Esquemas da AWS** está incorreta. A Ferramenta de Conversão de Esquemas da AWS normalmente é usada para migrações heterogêneas, nas quais você está migrando de um tipo de banco de dados para outro (por exemplo, Oracle para PostgreSQL). Nesse cenário, a migração é homogênea, ou seja, é uma migração de Oracle para Oracle. Como resultado, não há necessidade de converter o esquema, pois você permanece no mesmo tipo de banco de dados.

A opção que diz: **Migrar o banco de dados Oracle para um Amazon Aurora sem cluster com uma única instância** está incorreta. Embora um Aurora de instância única possa ser uma solução viável para aplicativos ou ambientes não críticos, como desenvolvimento ou teste, normalmente não é adequado para aplicativos que exigem alta disponibilidade.

Referências:

<https://aws.amazon.com/rds/details/multi-az/>

<https://aws.amazon.com/dms/>

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

Confira esta folha de dicas do Amazon RDS:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

60 . Pergunta

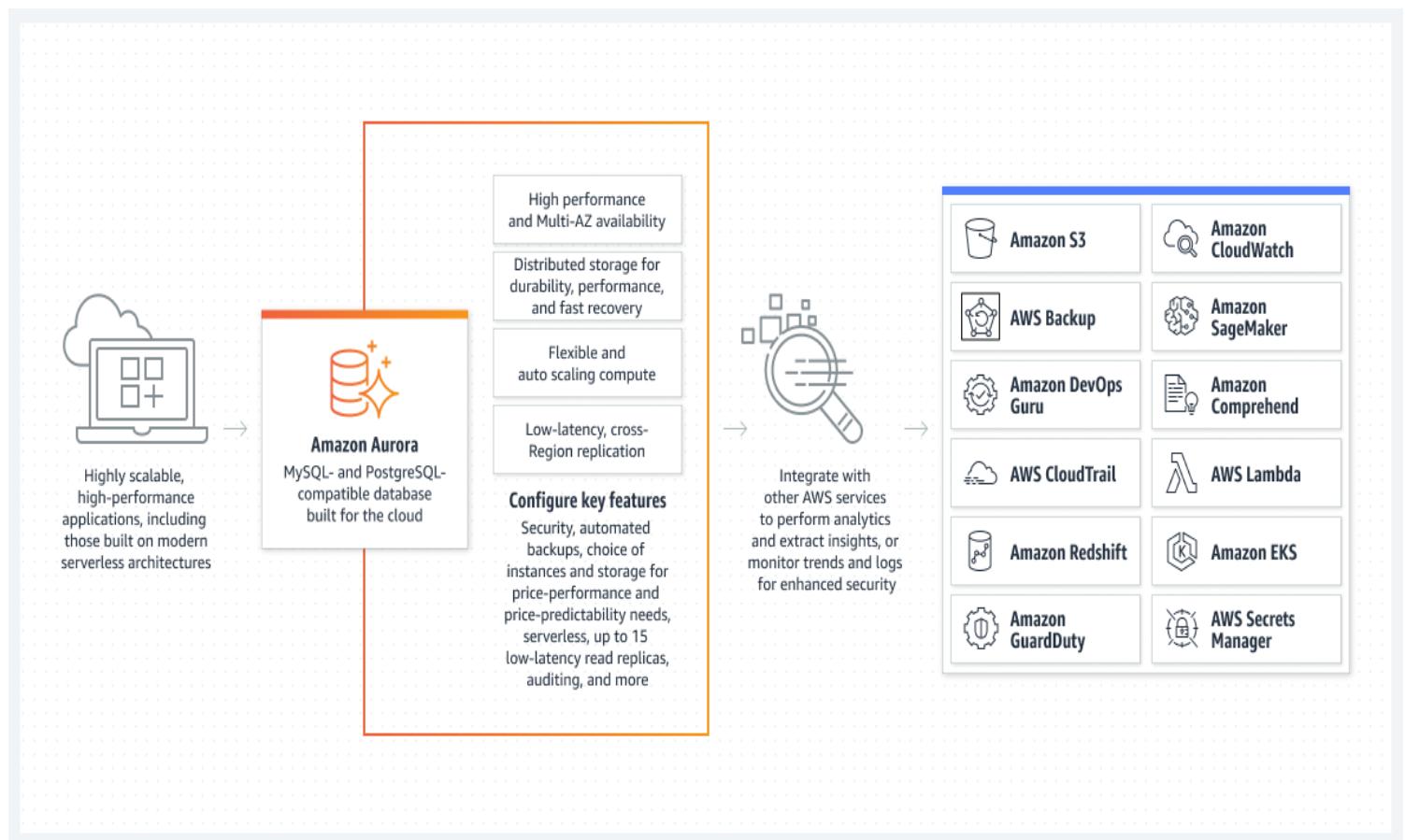
Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa de comércio eletrônico executa uma aplicação web altamente escalável que depende de um banco de dados Amazon Aurora. À medida que o número de usuários aumenta, a réplica de leitura enfrenta dificuldades para acompanhar o aumento do tráfego de leitura, causando gargalos de desempenho durante os períodos de pico.

Qual das seguintes opções resolverá o problema com a solução mais econômica?

Use o dimensionamento automático para a réplica de leitura do Aurora usando o Aurora Auto Scaling.

O **Amazon Aurora** é um serviço de banco de dados relacional baseado em nuvem que oferece melhor desempenho e confiabilidade para cargas de trabalho de banco de dados. Ele é altamente disponível e escalável, o que o torna uma ótima opção para empresas de qualquer porte. Um dos principais recursos do Amazon Aurora é o Aurora Auto Scaling, que ajusta automaticamente a capacidade do seu cluster de banco de dados Aurora com base na carga de trabalho. Isso significa que você não precisa se preocupar em ajustar manualmente a capacidade do seu cluster de banco de dados para lidar com mudanças na demanda. Com o Aurora Auto Scaling, você pode ter certeza de que seu cluster de banco de dados sempre terá a capacidade adequada para lidar com sua carga de trabalho, minimizando custos.



O Aurora Auto Scaling é particularmente útil para empresas com cargas de trabalho flutuantes. Ele garante que seu cluster de banco de dados seja dimensionado para cima ou para baixo conforme necessário, sem intervenção manual. Esse recurso economiza tempo e recursos, permitindo que as empresas se concentrem em outros aspectos de suas operações. O Aurora Auto Scaling também é econômico, pois ajuda a minimizar despesas desnecessárias associadas ao provisionamento excessivo ou insuficiente de recursos de banco de dados.

Nesse cenário, a empresa pode se beneficiar do uso do Aurora Auto Scaling. Essa solução permite que o sistema gerencie recursos dinamicamente, lidando efetivamente com o pico de tráfego de leitura durante os períodos de pico. Esse gerenciamento dinâmico de recursos garante que a empresa pague pelos recursos extras apenas quando eles forem realmente necessários.

Portanto, a resposta correta é: **Use o dimensionamento automático para a réplica de leitura do Aurora usando o Aurora Auto Scaling.**

A opção que diz: **Aumentar o tamanho do cluster de banco de dados Aurora** está incorreta, pois não é econômico aumentar o tamanho do cluster apenas para aliviar o gargalo durante os períodos de pico. Um aumento estático no tamanho do cluster de banco de dados resulta em custos constantes, independentemente de os recursos do seu banco de dados estarem sendo totalmente utilizados fora dos períodos de pico ou não.

A opção que diz: **Implementar escalonamento de leitura com o Aurora Global Database** está incorreta. O Amazon Aurora Global Database foi projetado principalmente para aplicativos distribuídos globalmente, permitindo que um único banco de dados Amazon Aurora abranja várias regiões da AWS. Embora isso possa fornecer disponibilidade global, introduz complexidade adicional e pode ser mais caro devido aos custos de infraestrutura e transferência de dados.

A opção que diz: **Configurar uma réplica de leitura que possa operar em diferentes regiões** está incorreta. Configurar uma réplica de leitura que opere em diferentes regiões pode proporcionar escalabilidade de leitura e benefícios de balanceamento de carga, distribuindo tipicamente o tráfego de leitura entre as regiões. No entanto, não é a solução mais econômica neste cenário, pois incorre em custos adicionais associados à replicação de dados entre regiões. Além disso, o problema não está relacionado à disponibilidade entre regiões, mas sim ao desempenho da réplica de leitura na região atual.

Referências:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScale.html>

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html

Confira esta folha de dicas do Amazon Aurora:

<https://tutorialsdojo.com/amazon-aurora/>

61 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas Seguras

Um sistema médico online hospedado na AWS armazena Informações Pessoais Identificáveis (PII) sensíveis dos usuários em um bucket do Amazon S3. Tanto as chaves mestras quanto os dados não criptografados nunca devem ser enviados à AWS para atender aos rigorosos requisitos regulatórios e de conformidade da empresa.

Qual técnica de criptografia S3 o arquiteto deve usar?

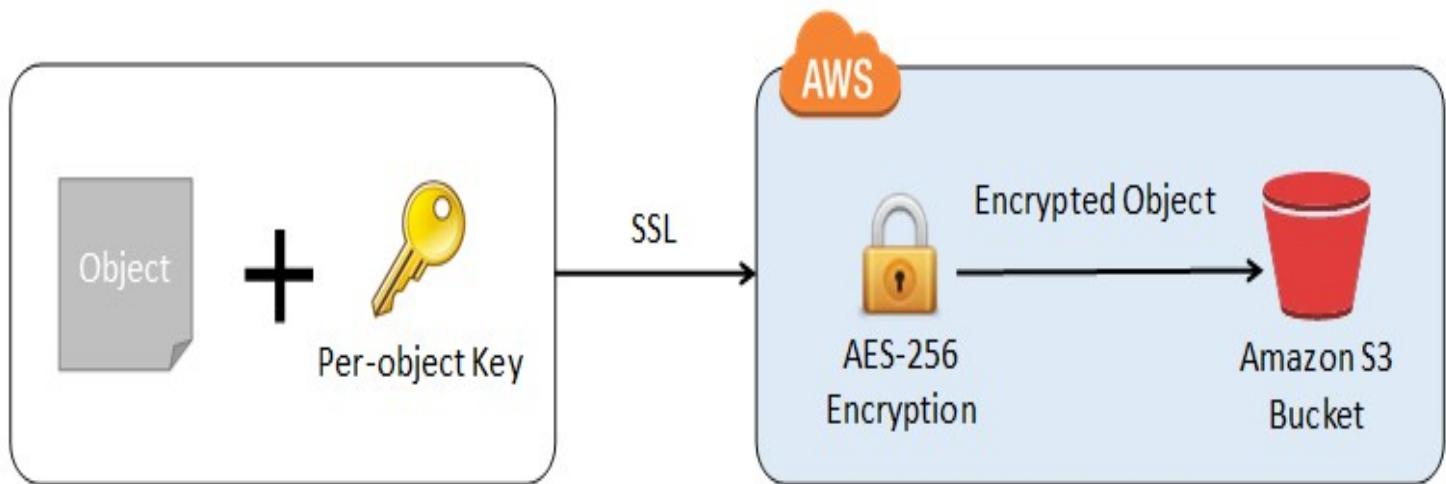
Use a criptografia do lado do cliente S3 com uma chave mestra do lado do cliente

A criptografia do lado do cliente é o ato de criptografar dados antes de enviá-los ao Amazon S3. Para habilitar a criptografia do lado do cliente, você tem as seguintes opções:

- Use uma chave AWS KMS.

- Use uma chave mestra do lado do cliente.

Ao usar uma chave KMS da AWS para habilitar a criptografia de dados do lado do cliente, você fornece um identificador de chave KMS da AWS (KeyId) à AWS. Por outro lado, ao usar uma chave mestra do lado do cliente para criptografia de dados do lado do cliente, suas chaves mestras do lado do cliente e seus dados não criptografados nunca são enviados à AWS. É importante que você gerencie suas chaves de criptografia com segurança, pois, se perdê-las, não será possível descriptografar seus dados.



É assim que funciona a criptografia do lado do cliente usando uma chave mestra do lado do cliente:

Ao carregar um objeto - Você fornece uma chave mestra do lado do cliente para o cliente de criptografia do Amazon S3. O cliente usa a chave mestra apenas para criptografar a chave de criptografia de dados que ele gera aleatoriamente. O processo funciona assim:

1. O cliente de criptografia do Amazon S3 gera uma chave simétrica de uso único (também conhecida como chave de criptografia de dados ou chave de dados) localmente. Ele usa a chave de dados para criptografar os dados de um único objeto do Amazon S3. O cliente gera uma chave de dados separada para cada objeto.

2. O cliente criptografa a chave de criptografia de dados usando a chave mestra fornecida por você. O cliente carrega a chave de dados criptografada e sua descrição do material como parte dos metadados do objeto. O cliente usa a descrição do material para determinar qual chave mestra do lado do cliente usar para a descriptografia.

3. O cliente carrega os dados criptografados no Amazon S3 e salva a chave de dados criptografada como metadados de objeto (`x-amz-meta-x-amz-key`) no Amazon S3.

Ao baixar um objeto - O cliente baixa o objeto criptografado do Amazon S3. Usando a descrição do material dos metadados do objeto, o cliente determina qual chave mestra usar para descriptografar a chave de dados. O cliente usa essa chave mestra para descriptografar a chave de dados e, em seguida, usa a chave de dados para descriptografar o objeto.

Portanto, a resposta correta é: **Use a criptografia do lado do cliente S3 com uma chave mestra do lado do cliente**.

A opção que diz: **Usar criptografia do lado do cliente S3 com uma chave KMS da AWS** está incorreta porque, na criptografia do lado do cliente com uma chave KMS, você fornece um identificador de chave KMS da AWS (KeyId) à AWS. O cenário indica claramente que tanto as chaves mestras quanto os dados não criptografados nunca devem ser enviados à AWS.

A opção que diz: **Usar criptografia do lado do servidor S3 com uma chave KMS da AWS** está incorreta porque o cenário mencionou que os dados não criptografados nunca devem ser enviados para a AWS, o que significa que você precisa usar a criptografia do lado do cliente para criptografar os dados antes de enviá-los para a AWS. Dessa forma, você só pode garantir que nenhum dado não criptografado seja carregado para a AWS. Além disso, a chave mestra usada pela Criptografia do Lado do Servidor com Chave KMS da AWS (SSE-KMS) é carregada e gerenciada pela AWS, o que viola diretamente o requisito de não carregar a chave mestra.

A opção que diz: **Usar criptografia do lado do servidor S3 com chave fornecida pelo cliente** está incorreta porque, como mencionado acima, você precisa usar criptografia do lado do cliente neste

cenário em vez de criptografia do lado do servidor. Para a criptografia do lado do servidor S3 com uma chave fornecida pelo cliente (SSE-C), você fornece a chave de criptografia como parte da sua solicitação para carregar o objeto no S3. Usando essa chave, o Amazon S3 gerencia tanto a criptografia (enquanto grava em discos) quanto a descriptografia (quando você acessa seus objetos).

Referências:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html>

Confira esta folha de dicas do Amazon S3:

<https://tutorialsdojo.com/amazon-s3/>

62 . Pergunta

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

Uma empresa está utilizando uma combinação de API Gateway e AWS Lambda para os serviços web de um portal online acessado por centenas de milhares de clientes diariamente. A empresa anunciará um novo produto revolucionário e espera-se que o portal receba um grande número de visitantes de todo o mundo. Como os sistemas e aplicativos de back-end podem ser protegidos contra picos de tráfego?

Usar limites de limitação no API Gateway

O Amazon API Gateway oferece limitação em vários níveis, incluindo global e por chamada de serviço. É possível definir limites de limitação para taxas e picos padrão. Por exemplo, os proprietários de APIs podem definir um limite de taxa de 1.000 solicitações por segundo para um método específico em suas APIs REST e também configurar o Amazon API Gateway para lidar com um pico de 2.000 solicitações por segundo por alguns segundos.



O Amazon API Gateway rastreia o número de solicitações por segundo. Quaisquer solicitações acima do limite receberão uma resposta HTTP 429. Os SDKs de cliente gerados pelo Amazon API Gateway realizam novas chamadas automaticamente ao receber essa resposta.

Portanto, a resposta correta é: **usar limites de limitação no API Gateway.**

A opção que diz: **O API Gateway escalará e lidará automaticamente com picos massivos de tráfego, para que você não precise fazer nada**, está incorreta. Embora ele possa escalar usando locais de borda da AWS, você ainda precisa configurar a limitação, normalmente para gerenciar melhor os picos de tráfego das suas APIs.

A opção que diz: **Atualizar manualmente as instâncias do Amazon EC2 usadas pelo API Gateway** está incorreta porque o API Gateway é um serviço totalmente gerenciado e, portanto, você não tem acesso aos seus recursos subjacentes.

A opção que diz: **Implantar Multi-AZ no API Gateway com Réplica de Leitura** está incorreta porque somente o RDS tem recursos de Multi-AZ e Réplica de Leitura, e não o API Gateway.

Referências:

https://aws.amazon.com/api-gateway/faqs/#Throttling_and_Caching

<https://docs.aws.amazon.com/apigateway/>

Confira esta folha de dicas do Amazon API Gateway:

<https://tutorialsdojo.com/amazon-api-gateway/>

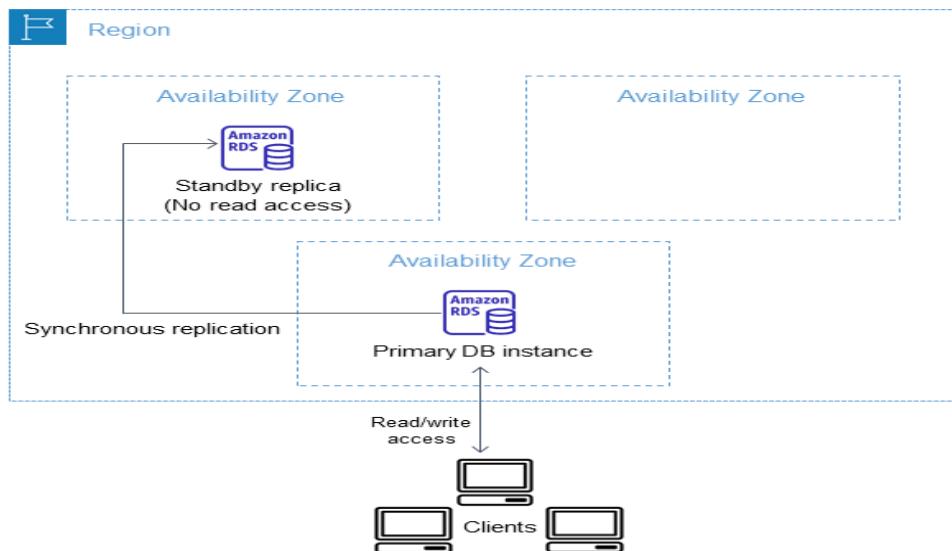
63 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Resilientes

Há muitas interrupções na Zona de Disponibilidade da sua instância do banco de dados RDS, a ponto de você perder o acesso ao banco de dados. O que você poderia fazer para evitar a perda de acesso ao seu banco de dados caso esse evento aconteça novamente?

Habilitar failover Multi-AZ

As implantações Multi-AZ do Amazon RDS oferecem disponibilidade e durabilidade aprimoradas para Instâncias de Banco de Dados (BD), tornando-as uma opção natural para cargas de trabalho de bancos de dados de produção. Para este cenário, **habilitar o failover Multi-AZ** é a solução correta. Ao provisionar uma Instância de Banco de Dados Multi-AZ, o Amazon RDS cria automaticamente uma Instância de Banco de Dados primária e replica os dados de forma síncrona para uma instância em espera em uma Zona de Disponibilidade (AZ) diferente. Cada AZ é executada em sua própria infraestrutura fisicamente distinta e independente, e foi projetada para ser altamente confiável.



Em caso de falha de infraestrutura, o Amazon RDS executa um failover automático para o standby (ou para uma réplica de leitura no caso do Amazon Aurora), para que você possa retomar as operações do banco de dados assim que o failover for concluído.

Criar um snapshot do banco de dados permite que você tenha um backup do seu banco de dados, mas não fornece disponibilidade imediata em caso de falha da AZ. Portanto, isso está .

Aumentar o tamanho da instância do banco de dados não é uma solução para este problema. Essa ação atende à necessidade de atualizar sua capacidade computacional, mas não resolve o requisito de fornecer acesso ao seu banco de dados mesmo em caso de perda de uma das Zonas de Disponibilidade.

Criar uma réplica de leitura é , pois isso simplesmente melhora o desempenho para cargas de trabalho de banco de dados com alto consumo de leitura. Embora seja possível promover uma réplica de leitura, sua replicação assíncrona pode não fornecer a versão mais recente do seu banco de dados.

Referência:

<https://aws.amazon.com/rds/details/multi-az/>

Confira esta folha de dicas do Amazon RDS:

<https://tutorialsdojo.com/amazon-relational-database-service-amazon-rds/>

Guia de estudo para o exame AWS Certified Solutions Architect Associate da Tutoriais Dojo:

<https://tutorialsdojo.com/aws-certified-solutions-architect-associate-saa-c02/>

64 . PERGUNTA

Categoria: CSAA - Design de Arquiteturas Seguras

Uma entidade governamental está realizando um censo populacional e habitacional na cidade. As informações de cada domicílio carregadas em seu portal online são armazenadas em arquivos criptografados no Amazon S3. O governo designou seu Arquiteto de Soluções para definir políticas de conformidade que verifiquem dados que contenham informações de identificação pessoal (PII) de forma a atender aos seus padrões de conformidade. Eles também devem ser alertados caso haja potenciais violações de política com relação à privacidade de seus buckets S3.

Qual das seguintes opções o arquiteto deve implementar para atender a esse requisito?

Configure e configure o Amazon Macie para monitorar seus dados do Amazon S3.

O **Amazon Macie** é um serviço de segurança com tecnologia de ML que ajuda a prevenir a perda de dados, descobrindo, classificando e protegendo automaticamente dados confidenciais armazenados no Amazon S3. O Amazon Macie usa aprendizado de máquina para reconhecer dados confidenciais, como informações de identificação pessoal (PII) ou propriedade intelectual, atribui um valor comercial e fornece visibilidade sobre onde esses dados estão armazenados e como estão sendo usados na sua organização.

The screenshot shows the AWS Macie console interface. On the left, there's a sidebar with navigation links: ALERTS, DASHBOARD, REPORTS, RESEARCH, SETTINGS, and INTEGRATIONS. The main area is titled 'Alerts (204)' and includes filters for 'Archived (277)' and 'All (481)'. A group archive section is also present. Three alert cards are displayed:

- S3 Bucket uses IAM policy to grant read rights to Everyone** (Severity 100)
 - Timestamp: 11 minutes ago
 - Comments: 0
 - Views: 0
 - Events: 1
- S3 Bucket uses IAM policy to grant read rights to Everyone** (Severity 100)
 - Timestamp: 21 minutes ago
 - Comments: 0
 - Views: 0
 - Events: 1
- Access Denied In Secure Account** (Severity 50)
 - Timestamp: 30 minutes ago
 - Comments: 0
 - Views: 0
 - Events: 27

O Amazon Macie gera duas categorias de descobertas: descobertas de políticas e descobertas de dados confidenciais. Uma descoberta de política é um relatório detalhado de uma possível violação de política ou problema com a segurança ou privacidade de um bucket do Amazon S3. O Macie gera essas descobertas como parte de suas atividades contínuas de monitoramento dos seus dados do Amazon S3. Uma descoberta de dados confidenciais é um relatório detalhado de dados confidenciais em um objeto do S3. O Macie gera essas descobertas quando descobre dados confidenciais em objetos do S3 que você configura uma tarefa de descoberta de dados confidenciais para analisar.

Portanto, a resposta correta é: **configurar e configurar o Amazon Macie para monitorar seus dados do Amazon S3**.

A opção que diz: **Configurar e configurar o Amazon Polly para verificar padrões de uso nos dados do Amazon S3** está incorreta porque o Amazon Polly é simplesmente um serviço que transforma texto em fala realista, permitindo criar aplicativos que falam e criar categorias inteiramente novas de produtos habilitados para fala. O Polly não pode ser usado para verificar padrões de uso nos seus dados do S3.

A opção que diz: **Configurar e configurar o Amazon Kendra para monitorar atividades maliciosas em seus dados do Amazon S3** está incorreta. O Amazon Kendra é apenas um serviço de pesquisa empresarial que permite aos desenvolvedores adicionar recursos de pesquisa aos seus aplicativos. Isso permite que seus usuários finais descubram informações armazenadas na vasta quantidade de conteúdo espalhado pela empresa, mas não monitorem atividades maliciosas em seus buckets do S3.

A opção que diz: **Configurar e configurar o Amazon Fraud Detector para enviar notificações de alerta sempre que uma violação de segurança for detectada nos dados do Amazon S3** está incorreta porque o Amazon Fraud Detector é apenas um serviço totalmente gerenciado para identificar atividades potencialmente fraudulentas e capturar mais fraudes online com mais rapidez. Ao contrário do Amazon Macie, ele não verifica nenhum dado do S3 que contenha informações de identificação pessoal (PII).

Referências:

<https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html>

<https://aws.amazon.com/macie/faq/>

<https://docs.aws.amazon.com/macie/index.html>

Confira esta folha de dicas da Amazon Macie:

<https://tutorialsdojo.com/amazon-macie/>

65 . PERGUNTA

Categoria: CSAA – Design de Arquiteturas de Alto Desempenho

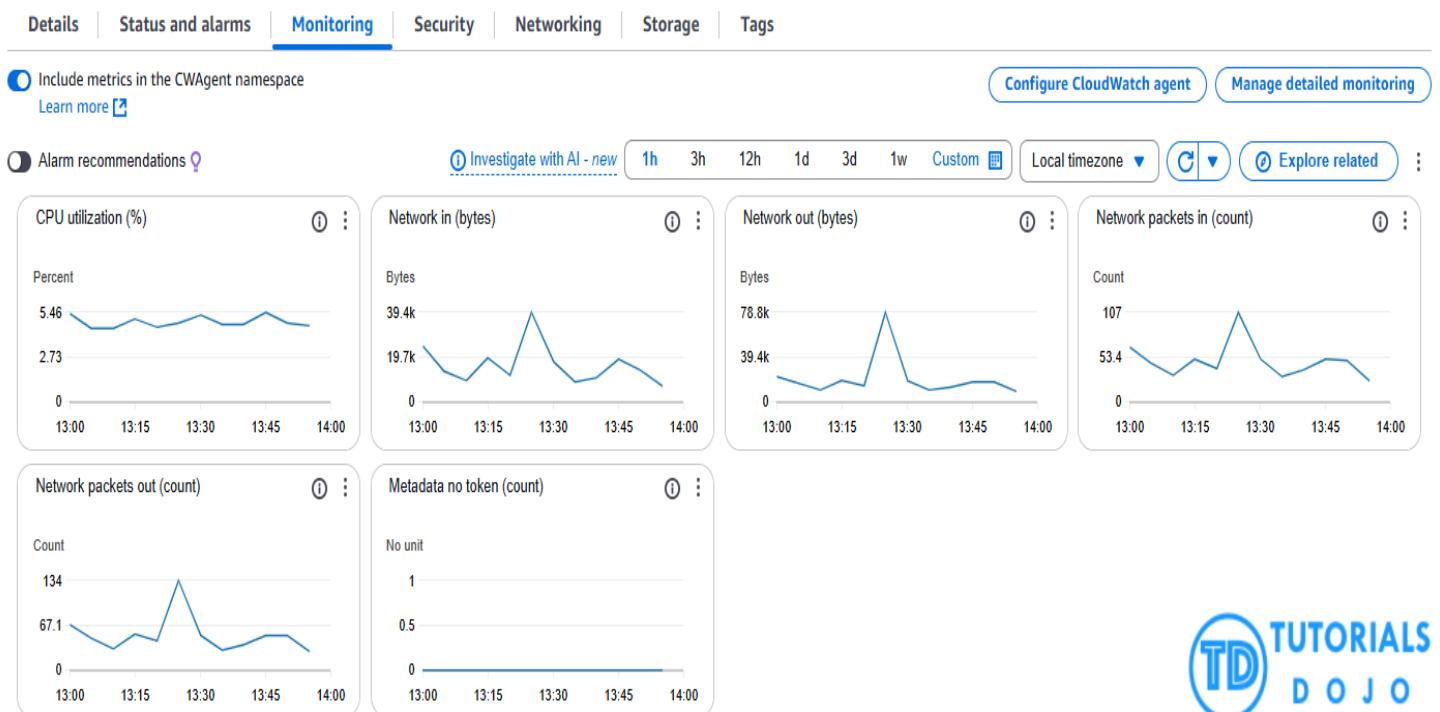
Uma empresa possui uma arquitetura de alta disponibilidade composta por um Elastic Load Balancer e várias instâncias do Amazon EC2 configuradas com Auto Scaling em três Zonas de Disponibilidade. A empresa precisa monitorar instâncias do EC2 com base em uma métrica específica que não está prontamente disponível no Amazon CloudWatch.

Qual das seguintes opções é uma métrica personalizada no CloudWatch que requer configuração manual?

Memory Utilization de uma instância EC2

O Amazon CloudWatch possui métricas do Amazon EC2 disponíveis para monitoramento. A utilização da CPU identifica a capacidade de processamento necessária para executar um aplicativo em uma instância selecionada. **Network Utilization** identifica o volume de tráfego de rede de entrada e saída para uma única instância. A **Disk Read** métrica é usada para determinar o volume de dados que o aplicativo lê do disco rígido da instância. Isso pode ser usado para determinar a velocidade do aplicativo. No entanto, existem certas métricas que não estão prontamente disponíveis no CloudWatch e que podem ser coletadas configurando uma métrica personalizada.

i-0612189812160kc (Kalayaan)



Você precisa preparar uma métrica personalizada usando os scripts de monitoramento do CloudWatch, escritos em Perl. Você também pode instalar o CloudWatch Agent para coletar mais métricas de nível de sistema de instâncias do Amazon EC2. Aqui está a lista de algumas das métricas personalizadas que você pode configurar:

- **Memory utilization**
- **Disk swap utilization**
- **Disk space utilization**
- **Page file utilization**
- **Log collection**

Portanto, a resposta correta é: **Memory Utilization** de uma instância EC2.

A opção que diz: **CPU Utilization** de uma instância EC2 está incorreta porque essa métrica normalmente está disponível por padrão no CloudWatch e não requer uma configuração de métrica personalizada.

A opção que diz: **Disk Read activity** de uma instância EC2 está incorreta porque apenas certas métricas relacionadas ao armazenamento, como **disk space utilization**, exigem monitoramento personalizado. Considerando que **disk read activity** já está incluído no CloudWatch.

A opção que diz: **Network packets out** de uma instância EC2 está incorreta porque essa métrica normalmente é incluída no monitoramento de utilização de rede padrão do CloudWatch, portanto, não há necessidade de configurar uma métrica personalizada.

Referências:

https://docs.aws.amazon.com/AwSEC2/latest/UserGuide/monitoring_ec2.html

https://docs.aws.amazon.com/AwSEC2/latest/UserGuide/mon-scripts.html#using_put_script

Confira estas folhas de dicas do Amazon EC2 e do Amazon CloudWatch:

<https://tutorialsdojo.com/amazon-elastic-compute-cloud-amazon-ec2/>

<https://tutorialsdojo.com/amazon-cloudwatch/>