1)

Além de serviços de IoT, os provedores de Computação em Nuvem oferecem soluções especializadas para outras áreas, como: serviços para Aprendizado de Máquina (*Machine Learning*); serviços para aplicações multimídia; e soluções para desenvolvimento de software.

Suponha que você queira criar máquinas virtuais para aplicações de segurança que envolvem o reconhecimento de faces de criminosos. O serviço mais indicado seria o

**Alternativas:**

* a)

Amazon SageMaker.

* b)

Deep Learning VM Image.

Alternativa assinalada

* c)

Azure Machine Learning.

* d)

AWS Elemental MediaConvert.

* e)

AWS Elemental MediaConnect.

2)

Os serviços voltados para aplicações que incluem conteúdo multimídia são muito importantes para facilitar o desenvolvimento de aplicações de streaming de vídeo, por exemplo.

De acordo com as informações apresentadas na tabela a seguir, faça a associação de alguns dos serviços para aplicações multimídia contidos na coluna A com suas respectivas descrições contidas na coluna B.

|  |  |
| --- | --- |
| **COLUNA A** | **COLUNA B** |
| I. *AWS Elemental MediaConvert*  II. *AWS Elemental MediaConnect*  III. *Live and on- demand streaming*  IV. *Content Protection* | 1. Serviço com recursos para codificação e distribuição escalável de vídeo (ao vivo ou sob demanda).    2.  Solução para transmissão de vídeo ao vivo escalável, confiável e segura.    3.   Mecanismos de criptografia e gerenciamento de direitos autorais para mídias digitais a fim de proteger conteúdo distribuído na Internet.    4. Mecanismos para converter um vídeo de entrada em diferentes formatos de saída a fim de oferecer suporte para várias plataformas e dispositivos. |

Assinale a alternativa que apresenta a associação CORRETA.

**Alternativas:**

* a)

I-2, II-1, III-3, IV-4.

* b)

I-4, II-3, III-1, IV-2.

* c)

I-3, II-2, III-4, IV-1.

* d)

I-4, II-2, III-1, IV-3.

Alternativa assinalada

* e)

I-1, II-4, III-2, IV-3.

3)

Um dos tipos de servic¸o de armazenamento em Nuvem e´ o armazenamento de bases de dados. Esse modelo corresponde aos servic¸os de banco de dados em Nuvem ou Banco de dados como Servic¸o (DBaaS - Database as a Service). Sa~o servic¸os que, em geral, suportam algum tipo de linguagem de consulta ale´m de operac¸o~es ba´sicas de escrita ou leitura de dados.

Considerando o conceito e a utilização de bancos NoSQL, analise o excerto a seguir, completando suas lacunas.

O baixo desempenho dos bancos de dados \_\_\_\_\_\_\_\_\_\_\_\_ para gerenciamento de grandes volumes de dados motivou o desenvolvimento dos bancos de dados \_\_\_\_\_\_\_\_\_. Os bancos na~o relacionais apresentam desempenho e escalabilidade significativamente superior para lidar com grandes volumes de dados \_\_\_\_\_\_\_\_\_\_\_\_, o que e´ muito importante, por exemplo, para aplicac¸o~es web em larga escala.

Assinale a alternativa que preenche corretamente as lacunas.

**Alternativas:**

* a)

relacionais / não relacionais / não estruturados.

Alternativa assinalada

* b)

não relacionais / relacionais / estruturados.

* c)

não relacionais / relacionais / não estruturados.

* d)

normais / anormais / desestruturados.

* e)

anormais /  normais / estruturados.

4)

Os mecanismos de segurança devem ser usados em conjunto e aprimorados continuamente para lidar com eventuais ações maliciosas contra as aplicações em ambientes de Nuvem. Os principais mecanismos de segurança disponíveis para computação em Nuvem são: criptografia, gerenciamento de acesso e identidade, autenticação unificada e imagens fortalecidas de máquinas virtuais.

De acordo com as informações apresentadas na tabela a seguir, faça a associação dos mecanismos de segurança que podem ser aplicados à computação em nuvem contidos na Coluna B com suas respectivas características respectivos, apresentadas na Coluna A.

|  |  |
| --- | --- |
| **COLUNA A** | **COLUNA B** |
| I.              É importante na implementação de soluções de segurança para lidar com ataques de negação de serviços, autenticação fraca e violação de privacidade no acesso a dados e serviços. | 1 - Criptografia |
| II.            São configuradas por especialistas considerando as políticas de segurança rigorosas para se eliminar possível vulnerabilidades. | 2 - Gerenciamento de acesso e identidade |
| III.           Utiliza algoritmos para verificar a integridade dos dados, além de ser usado em mecanismos de assinatura digital. |
| IV.          São mecanismos que oferecem uma solução segura para autenticação em vários provedores utilizando as mesmas credenciais. | 3 - Autenticação unificada |
| V.            Consiste em técnicas que permitem disfarçar os dados enviados de forma que um atacante não consiga obter nenhuma informação dos dados interceptados. | 4 - Imagens fortalecidas de máquinas virtuais |

Assinale a alternativa que apresenta a associação CORRETA entre as colunas.

**Alternativas:**

* a)

I - 4; II - 2; III - 3; IV - 2; V - 1.

* b)

I -2; II - 4; III - 1; IV - 3; V - 1.

Alternativa assinalada

* c)

I - 1; II - 2; III - 3; IV - 4; V - 1.

* d)

I - 2; II - 1; III - 4; IV - 3; V - 1.

* e)

I - 3; II - 4; III - 1; IV - 2; V - 1.

5)

A criptografia consiste em técnicas que permitem disfarçar os dados enviados de forma que um atacante não consiga obter nenhuma informação dos dados interceptados. A criptografia pode ser usada em mecanismos para garantia de confidencialidade, integridade e autenticidade. Existem duas abordagens para codificar os dados de modo que somente o destinatário legítimo poderá decifrar esses dados: a criptografia de chaves simétricas e a criptografia de chave pública.

Com relação a criptografia na computação em nuvem, analise as afirmativas a seguir.

I. Na criptografia de chaves simétricas existe um par de chaves que é utilizado pelo remetente para criptografar os dados que serão enviados ou armazenados em Nuvem.

II. Na abordagem de criptografia de chave pública, o processo envolve um par de chaves. O remetente precisa gerar uma chave pública para enviar os dados, e para o destinatário receber os dados, ele precisa gerar o seu par de chaves.

III. Comparada com a abordagem criptografia de chave pública, a criptografia de chaves simétricas tem a vantagem de exigir menos capacidade computacional na criptografia dos dados.

IV. A criptografia de chaves públicas é usada somente para compartilhar com segurança uma chave única entre o remetente e o emissor que, então, usam essa chave única para transmitir os dados por meio de criptografia de chave simétrica.

Considerando o contexto apresentado, é correto o que se afirma em:

**Alternativas:**

* a)

I e II, apenas.

* b)

III e IV, apenas.

Alternativa assinalada

* c)

I, II e III, apenas.

* d)

I, III e IV, apenas.

* e)

I, II, III e IV.