

Sistemas Distribuídos, 2017/18 - 1º MINI Teste

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.

Cada resposta de escolha múltipla errada desconta 1/4 da sua cotação.

No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ **Nome:** _____

- 1) A tolerância a faltas de um sistema distribuído, quando comparado com uma alternativa não distribuída, pode ser:
- A. Melhor, porque um sistema distribuído pode replicar máquinas;
 - B. Pior, porque há mais pontos de falha na alternativa distribuída que na não-distribuída;
 - C. Pior, porque há mais tipos de faltas possíveis;
 - D. Todas as anteriores.

- 2) Considere o protocolo de *primary backup*. O que pode ser uma falta arbitrária (ou bizantina)?
- A. O primário atualiza o estado e não envia a mensagem ao secundário.
 - B. O tempo de propagação do $l'm$ alive excede o valor de t_{max} .
 - C. O cliente contacta o secundário e este executa a operação pedida.
 - D. Todas as acima.

- 3) O protocolo *primary-backup* pressupõe que o tempo máximo de entrega de uma mensagem na rede (t_{max}) existe e é pré-conhecido. À medida que o limite t_{max} decresce, que métrica consigo melhorar?
- A. O tempo médio entre falhas do sistema.
 - B. O tempo médio para recuperar o sistema.
 - C. O grau de replicação.
 - D. Nenhuma métrica é afetada.

- 4) Num sistema de 3 réplicas que usa o protocolo quorum consensus (pesos idênticos, quóruns de maioria), o estado das réplicas num dado instante é o seguinte (seq – sequence number, cid – client identifier):

Réplica A: valor = 18; tag = {seq=5, client-id=1}

Réplica B: valor = 15; tag = {seq=6, client-id=4}

Réplica C: valor = 13; tag = {seq=7, client-id=5}

Caso um cliente tente ler o valor replicado, que valor retorna?

- A. Valor 13
- B. Valor 15
- C. Valor 13 ou 15, dependendo das réplicas que respondam primeiro.
- D. Valor 18

- 5) Num sistema replicado por *quorum consensus*, um dos gestores de réplica recebeu (por esta ordem) estes pedidos de escrita: $\langle v1, \langle seq=1, client-id=3 \rangle \rangle$; $\langle v3, \langle seq=3, client-id=3 \rangle \rangle$; $\langle v2, \langle seq=2, client-id=1 \rangle \rangle$. Qual o valor final que a réplica armazena?

- A. v1
- B. v2
- C. v3
- D. Nenhum dos anteriores

6) "Os dados da aplicação podem ser interceptados na rede através de uma vulnerabilidade do HTTPS."

A afirmação define:

- A. Uma política de segurança
- B. Um mecanismo de segurança
- C. Uma ameaça de segurança
- D. A e C.

7) Qual é a vulnerabilidade conhecida do algoritmo DES?

- A. Possibilidade de utilização de diferentes modos de combinação de blocos.
- B. Tamanho do bloco de cifra.
- C. Chave de pequena dimensão.
- D. Necessidade de enchimento (padding) do último bloco de dados.

8) Um servidor SSH protegido por Kerberos recebe um pedido juntamente com um *ticket*. O *ticket* permite ao servidor:

- A. Receber chave de sessão gerada pelo cliente.
- B. Receber chave de sessão gerada pelo Saut
- C. Verificar que a sua hora atual está sincronizada com o Saut.
- D. A e B.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Total |
|-----|-----|-----|-----|-----|-----|-----|-----|------------|
| 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 2,5 | 20 valores |

DDBCCCB