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) No modelo de sistema assíncrono.
   A. Os pressupostos aproximam-se mais da realidade do que num sistema síncrono, em particular se houver uma partição na rede, ou um ataque de "denial-of-service".
   B. É possível a deteção remota de falhas por paragem (*crash failures*).
   C. Pode considerar-se a existência de um limite superior no tempo de latência da rede.
   D. Nenhuma das anteriores é válida.

   [ ]

2) Comparando um sistema replicado com *primary-backup* com outro que recorre a *quorum consensus*, ambos dimensionados para tolerar *f* gestores de réplica em falha:

   A. O *primary-backup* exige menos réplicas, mas o *quorum consensus* coloca menos restrições sobre a rede na qual funcionará.
   B. O *quorum consensus* exige menos réplicas, mas o *primary-backup* coloca menos restrições sobre a rede na qual funcionará.
   C. O *primary-backup* exige menos réplicas e coloca menos restrições sobre a rede na qual funcionará.
   D. O *quorum consensus* exige menos réplicas e coloca menos restrições sobre a rede na qual funcionará

   [ ]

3) Num sistema de réplica passiva o secundário espera a receção da mensagem de prova de vida que ainda não chegou (P é o período entre provas de vida e Tmax é o tempo máximo de propagação na rede).
   A. Ao fim de P+tmax avisa o primário que o vai substituir.
   B. Ao fim de P+3tmax inicia o processo de substituir o primário porque tenta ainda verificar se este está em baixo antes de substitui-lo.
   C. Ao fim do período P inicia o processo de substituir o primário.
   D. Ao fim de P+tmax inicia o processo de substituir o primário.

   [ ]

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}
   A. Este estado não é possível neste protocolo.
   B. Há pelo menos uma escrita que está ainda em curso.
   C. Ocorreram escritas concorrentes.
   D. Nenhuma das anteriores.

   [ ]

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

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

[ ]

6) "Os dados da aplicação são cifrados com AES-256 antes de serem guardados numa base de dados."
A afirmação define:

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

[ ]

7) Pretende-se garantir **apenas** a *integridade* de uma mensagem M que vai ser transmitida numa rede insegura. Existe uma chave K partilhada pelo emissor e recetor. Estão disponíveis as seguintes funções criptográficas: CifraAES, CifraDES, DecifraAES, DecifraDES, SHA2, HmacSHA2, MD5, HmacMD5 .

A. Enviar: M, HmacSHA2(M, K)
B. Enviar: CifraAES(M,K), HmacSHA2(M, K)
C. Enviar: M, CifraAES(SHA2(M), K).
D. A e C são ambas corretas, mas a opção C é computacionalmente mais pesada.

[ ]

8) No Kerberos, considere um ticket para o cliente C usar o serviço S:

A. O ticket é seguro porque é cifrado com a chave pública do servidor S
B. O ticket é seguro porque é cifrado com uma chave que é um segredo entre o Kerberos e o servidor S
C. O ticket é seguro porque é cifrado com a chave do cliente
D. O ticket é seguro porque a chave KC,S é gerada pelo Kerberos e só este a conhece

[ ]

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**

A A D B C D D B