LETI/LEIC 2017/18, 2º Teste de Sistemas Distribuídos

19 de junho de 2018

Responda no enunciado, usando apenas o espaço fornecido. Identifique todas as folhas.
Uma resposta errada numa escolha múltipla desconta 1/N do valor da pergunta em N alternativas.
Duração da prova: 1h30m

Grupo I [7 valores]

1) [0,8v] Considere um sistema replicado que, segundo um qualquer protocolo de replicação, mantém um valor inteiro replicado. Dois clientes concorrentes, P1 e P2, executaram as seguintes operações sobre a **mesma** variável deste sistema:
   Inicialmente o valor replicado era 0 (zero).
   P1 executou (por esta ordem): write(2); write(3);
   P2 executou (por esta ordem): read()->3; read()->2;
   Este sistema é sequencialmente consistente? Justifique.

2) Considere que uma empresa de compras online oferece um *web service* que permite aos seus clientes consultar o catálogo e efetuar encomendas. Este web service é alojado num servidor que é replicado segundo o protocolo *primary-backup* estudado nas aulas teóricas.
   Existem dois servidores, S1 e S2, ambos localizados na mesma rede local. Nessa rede existe também um servidor UDDI que permite aos clientes descobrirem qual dos dois servidores é atualmente o primário.

   a) [1,0v] Um cliente chamou a função *checkout*, que efetua a encomenda contida no carrinho de compras de um utilizador. O único argumento da chamada foi identificador de utilizador *1234* e, como retorno, a chamada devolveu o identificador de encomenda 142018.
   Complete o diagrama abaixo com as mensagens trocadas entre cliente e servidores, assumindo que o cliente tem já conhecimento que o servidor primário é o S1 e que não ocorrem falhas durante a chamada.
   Seja claro quanto ao conteúdo de cada mensagem. Pode omitir as mensagens de prova de vida (*I'm alive*).

b) Considere ainda a chamada a *checkout*. Para cada uma das situações patológicas abaixo, indique se esta pode ocorrer neste sistema replicado ou não. Se sim, ilustre com um exemplo; se não, justifique indicando sucintamente os mecanismos que previnem cada situação.

i) [0,8v] Como o servidor primário falhou antes de propagar a atualização de estado ao secundário, o cliente pensará que a encomenda foi efetuada mas o estado do sistema perdeu essa informação.

Pode ocorrer / Não pode ocorrer.

ii) [0,8v] Como o servidor primário propagou a atualização do seu estado ao secundário mas falhou antes de devolver a resposta ao cliente, o secundário efetuou duas encomendas.

Pode ocorrer / Não pode ocorrer.

3) Nas seguintes alíneas, considere um sistema replicado por *quorum consensus* com 5 réplicas num instante em que o estado do sistema é:
   - R1: <val=10; <seq=4; cid=1>>
   - R2: <val=10; <seq=4; cid=1>>
   - R3: <val=20; <seq=5; cid=2>>
   - R4: <val=20; <seq=5; cid=2>>
   - R5: <val=10; <seq=4; cid=1>>

a) [0,9v] Se um cliente ler do sistema neste momento e receber respostas das réplicas R1, R2 e R3, que valor retornará?
   i) 10
   ii) 20
   iii) Pode ser 10 ou 20
   iv) Nenhuma das opções acima.

b) [0,9v] [0,8v] Considerando agora qualquer possível conjunto de respostas (ou seja, qualquer quórum de respostas), que valores podem ser lidos por um cliente que tente ler?
   i) 10
   ii) 20
   iii) Pode ser 10 ou 20
   iv) Nenhuma das opções acima.

c) [0,9v] Assumindo que todas as mensagens em trânsito na rede chegam ao seu destino, que não ocorrem falhas e que nenhum cliente submete nenhuma nova escrita no sistema, qual o estado em que ficarão todas as réplicas?
   i) Todas as réplicas com <val=10; <seq=4; cid=1>>
   ii) Todas as réplicas com <val=20; <seq=5; cid=2>>
   iii) O estado descrito acima mantém-se
   iv) Nenhuma das anteriores

d) [0,9v] Considere uma variante hipotética do protocolo *quorum consensus* em que os quóruns (para escrita e leitura) passam a ser ambos de 1/3 das réplicas (em vez de quóruns de maioria). Apresente uma vantagem e uma desvantagem desta variante (relativamente ao protocolo original).

Vantagem:
Desvantagem:

Grupo II [3 valores]

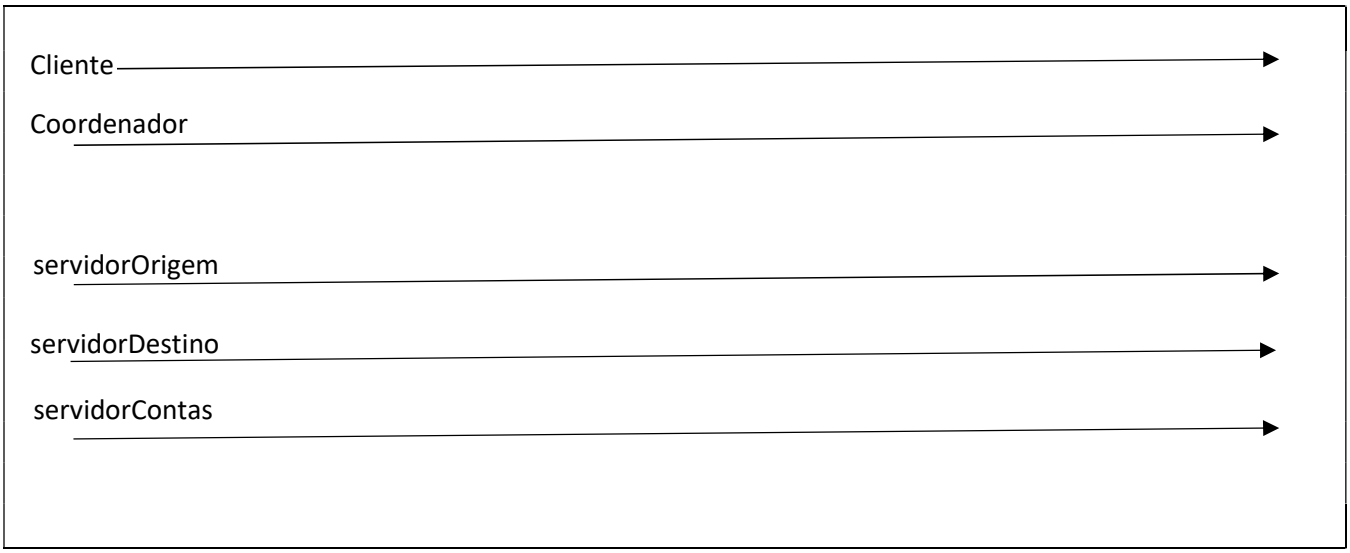
Num sistema de *bike-sharing*, existem diferentes servidores: desde os servidores que gerem cada estação de bicicletas aos servidores que mantêm as contas de utilizadores.
Num destes sistemas, considere que existia a operação levantarComReserva, que executa três operações em servidores distintos de forma atómica, recorrendo a uma transação distribuída. A operação é definida da seguinte forma:

```
1 levantarComReserva (string utilizador, int estacaoOrigem, int estacaoDestino) {
2     servidorOrigem = lookup(estacaoOrigem);
3     servidorDestino = lookup(estacaoDestino);
4     servidorContas = lookup("utilizadores");

5     idDTx = coord.openTransaction();
6     try {
7           servidorOrigem.levantarBicicleta(utilizador, idDTx);
8           servidorDestino.reservarVaga(utilizador, idDTx);
9           servidorContas.debitar(utilizador, TAXA_RESERVA, idDTx);
10          coord.closeTransaction(idDTx);
11    } catch (Exception e) {
12          coord.abortTransaction(idDTx);
      }
}
```

1) [0,9v] Numa situação em que o programa chega à linha 10, quantas transações locais foram criadas nos servidores participantes? Para cada transação, indique a linha do programa em que ela foi criada.

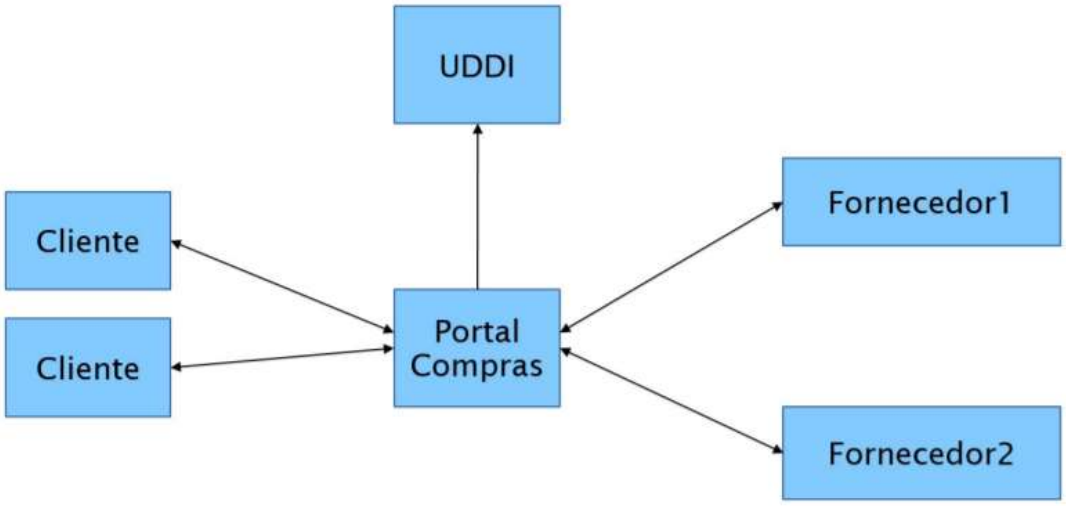
2) [1,2v] Considere que o programa chegou à linha 10 e o coordenador iniciou o protocolo 2-Phase Commit (2PC) para confirmar a transação distribuída. Complete o diagrama seguinte com todas as mensagens trocadas pelo 2PC. Considere que o coordenador vai receber um voto NÃO do servidorDestino.



3) [0,9v] Se, na situação da alínea anterior, o voto NÃO se tivesse atrasado para além do limite razoável, o que teria decidido o coordenador?
   A. Após um tempo razoável, decidia cancelar.
   B. Após um tempo razoável, decidia confirmar.
   C. Não podia decidir, tinha obrigatoriamente de esperar pela mensagem atrasada.
   D. Não disponho da informação necessária para responder de forma concreta.

Grupo III [10 valores]

Considere um sistema de *Web Services* composto por um portal de compras e um conjunto de fornecedores. Os clientes pesquisam no portal por produtos que são vendidos pelos fornecedores.



O servidor UDDI é usado pelo Portal e pelos Fornecedores para registarem o seu nome, endereço e informação de negócio, através da operação *publish()*. O servidor UDDI é usado pelos Clientes e pelo Portal para pesquisar pelos serviços com a operação *query()*. Na imagem acima apenas é representada a comunicação do Portal de Compras com o UDDI.

Toda a comunicação usa o protocolo HTTP e mensagens SOAP sem qualquer proteção. O sistema está em funcionamento, mas entretanto surgiram preocupações…

1) [0,8v] Das seguintes opções, qual é a ameaça concreta ao sistema a ter em conta?
   A. Um fornecedor malicioso pode registar-se no sistema.
   B. Um cliente malicioso pode fazer uma compra em nome de outro cliente.
   C. Um fornecedor malicioso pode intercetar as respostas de outro fornecedor e aumentar os preços.
   D. Todas as anteriores.

   [ ]

2) [0,9v] Proponha uma política de segurança a introduzir para o sistema passar impedir uma ameaça concreta à qual este sistema esteja vulnerável (no caso de encontrar múltiplas ameaças, escolha uma).

Ameaça:
Política:

3) Assuma agora que para a proteção do sistema, dispõe apenas das seguintes funções criptográficas: DES, AES128, MD5, SHA1, SHA2.

   a) [0,8v] Qual é a afirmação correta?

   A. DES, AES128 e MD5 são cifras simétricas, SHA1 e SHA2 são funções de resumo.
   B. DES, AES128 são cifras simétricas, MD5, SHA1, SHA2 são funções de resumo
   C. DES e AES128 são cifras assimétricas, MD5, SHA1, SHA2 são funções de resumo.
   D. AES128 é uma cifra simétrica, as restantes são funções de resumo.

   [ ]

   b) [0,8v] Qual é a diferença entre um HMAC e uma função de resumo?

   A. Um HMAC é uma função de resumo mas baseada em criptografia assimétrica.
   B. Um HMAC é uma função de resumo mas baseada em criptografia híbrida.
   C. Um HMAC é uma versão mais rápida de uma função de resumo.
   D. Um HMAC é um resumo chaveado, ou seja, é uma função de resumo que também usa um segredo.

   [ ]

c) Adicionou-se ao sistema um servidor de autenticação Kerberos (considere o protocolo simplificado ensinado nas aulas teóricas).

Antes do sistema se iniciar, fez-se a seguinte distribuição de chaves secretas (onde K_x é a chave de X):

Portal: K_p, Fornecedor 1: K_{f1}, Fornecedor 2: K_{f2}, UDDI: K_{uddi}, Saut: {K_p, K_{f1}, K_{f2}, K_{uddi}}

i) [0,9v] Como pode o Fornecedor 1 obter uma chave para "falar" com o UDDI ($K_{f1,uddi}$)? Indique o emissor, recetor e conteúdo de cada mensagem trocada.

ii) [1,0v] Proponha agora uma proteção a aplicar à mensagem SOAP, do pedido de *publish(),* enviado pelo Fornecedor1 para o UDDI de modo a garantir apenas a integridade das mensagens. Escolha os algoritmos mais seguros à sua disposição.

4) Assuma agora que dispõe também da função criptográfica: RSA-2048.

a) [0,8v] Que tipo de algoritmo é o RSA? A que se refere o número 2048?

A. RSA é um algoritmo de cifra assimétrica, 2048 é o tamanho da chave (em bits).
B. RSA é um algoritmo de cifra simétrica, 2048 é o tamanho da chave (em bits).
C. RSA é um algoritmo de cifra assimétrica, 2048 é o expoente da chave (em bits).
D. RSA é um algoritmo de cifra simétrica, 2048 é o tamanho do bloco (em bits).

b) Adicionou-se um servidor de autoridade de certificação (CA) e retirou-se o servidor Kerberos.

Antes do sistema se iniciar, fez-se a seguinte distribuição de chaves (onde K_{pub_X} é a chave pública de X, K_{priv_X} é a chave privada de X):

Portal: K_{priv_p} K_{pub_ca}, Fornecedor 1: K_{priv_f1} K_{pub_ca}, Fornecedor 2: K_{priv_f2} K_{pub_ca}
UDDI: K_{priv_uddi} K_{pub_ca}, CA: K_{priv_ca}, K_{pub_p}, K_{pub_f1}, K_{pub_f2}, K_{pub_uddi}

Para garantir a autenticidade e a integridade das mensagens de pedidos, estas passam a ser protegidas com uma **assinatura digital** usando RSA. Use como exemplo uma mensagem de pedido enviada pelo Fornecedor2 para o UDDI.

i) [0,8v] Como pode uma chave pública ser distribuída de forma confiável?

ii) [0,8v] Como é calculada a assinatura digital de um pedido? Detalhe os passos.

iii) [0,8v] Como pode o recetor de uma mensagem transportando uma assinatura digital confirmar que a mensagem foi de facto emitida pelo emissor nela indicado (e não por um impostor)? Justifique.

iv) [0,8v] Uma assinatura digital deve ser protegida contra *replay attack*. Indique uma proteção e justifique como impede o ataque.

5) [0,8v] Compare agora a utilização de Kerberos com a utilização de uma CA. Indique uma vantagem de cada.

Vantagem Kerberos:
Vantagem CA: