LETI/LEIC 2017-18, Exame de Época Especial de Sistemas Distribuídos

25 de julho de 2018

Responda no enunciado, usando apenas o espaço fornecido. Identifique todas as folhas.
Uma resposta errada numa escolha múltipla com N opções desconta 1/N do valor da pergunta.
Duração da prova: 2h30m

Grupo I [3,5v]

Considere a seguinte IDL do Sun RPC de um serviço semelhante ao Doodle, que permite a um grupo de pessoas escolherem (por votação) uma entre múltiplas opções de datas para um evento.

A interface deste serviço fornece apenas um método remoto, descrito abaixo na IDL do SUN RPC. O método permite ao cliente votar numa das opções disponíveis para um evento. O servidor retorna ao cliente os votos totais dessa mesma opção (acumulados até ao momento). A implementação do método no servidor é idempotente.

```
enum vote_error {
   CALL_OK = 0,              /* No error */
   CALL_ID_NOT_FOUND = 1     /* Suggestion ID not found */
};
struct vote_args {
    long idVote;
    long idEvent;
    long idOption;
};
struct vote_result {
    vote_error error;
    double numVotes;
};
program VOTE_PROG {
    version VOTE_VERS {
        vote_result POSTVOTE(vote_args);
    };
} = 100400;
```

1. [0,7v] Considere a seguinte implementação (em pseudo-código) da função postVote no servidor.

```
vote_result *postVote(idVote, idEvent, idOption) {
    event* event = events[idEvent];
    event->options[idOption].voteCount++;
    return event->options[idOption].voteCount;
}
```

Esta implementação é idempotente? Justifique.

2. [0,7v] Com base nestes parâmetros ilustre com um exemplo o problema da heterogeneidade numa arquitetura distribuída.

3. [0,6v] Considere que este serviço de votação está disponibilizado em vários servidores. Pretende-se que a aplicação cliente se ligue a cinco destes servidores, e que selecione alternadamente a ligação a utilizar para cada pedido de invocação remota.
   Será possível o programador da aplicação cliente cumprir este requisito? Justifique.

4. Para cada situação descrita de seguida, indique em qual **semântica(s) de execução** esta se pode verificar e apresente uma explicação.
   a. [0,5v] Num sistema que garante que as mensagens são entregues ao fim de 1 ms (exceto casos de perdas) e que a execução local de uma função no servidor demora no máximo 100 ms, um cliente chamou POSTVOTE e só recebeu resposta ao fim de 5 s.

Semântica(s):

   b. [0,5v] Um cliente chamou a variante não idempotente de POSTVOTE; mais tarde veio a saber que o seu voto foi erradamente considerado em duplicado.

Semântica(s):

   c. [0,5v] Um cliente invocou POSTVOTE mas o servidor falhou a meio da execução, deixando o seu estado interno incoerente. O stub devolveu erro de RPC ao cliente e o servidor, após recuperar, anulou as alterações, regressando a um estado coerente.

Semântica(s):

Grupo II [3v]

Considere o seguinte programa de um cliente, programado em Java, que recorre a sockets UDP para invocar uma operação remota que regista um novo utilizador num servidor, programado noutra linguagem de programação.

```
class Cliente {
   public static void main(String args[]) throws Exception
   {
      String nomeServidor = "exemplo.sd.tecnico.ulisboa.pt";
      int portoServidor = 3456;
      DatagramSocket s = new DatagramSocket();
      InetAddress enderecoIP = InetAddress.getByName(nomeServidor);

      //Argumentos do pedido
      String nome = "José Silva";
      int idade = 30;
      int codigoPostal = 1230;

      //Identificador da operação *regista*
      int op = 1;

      //Serializa o id de operacao e argumentos num array de bytes
      byte[] pedido = ...

      DatagramPacket pacotePedido =
          new DatagramPacket(pedido, pedido.length, enderecoIP, portoServidor);
      s.send(pacotePedido);
      DatagramPacket pacoteResposta =
          new DatagramPacket(pacoteResposta, pacoteResposta.length);
      s.receive(pacoteResposta);

      //Desserializa a resposta
      int resposta = ...

      System.out.println("Resposta recebida: " + resposta);
      s.close();
}}
```

1. [0,6v] Pretende-se portar este sistema para Java RMI. Com base na informação no código acima, componha a interface remota correspondente. Caso o código acima não lhe dê informação suficiente para conhecer alguns elementos da interface, escolha-os livremente.

2. [0,6v] Programe agora um cliente que obtém uma referência para uma instância da referência remota definida na alínea anterior e faz uma chamada remota com efeitos equivalentes àqueles do programa com sockets. Assuma que a instância remota se encontra registada com o nome "sd.tecnico.ulisboa.pt/exemplo".
   Simplificação: omita do seu programa a definição do SecurityManager.

3. Para cada afirmação abaixo, indique se a afirmação é verdadeira ou falsa para cada variante do sistema (Java/sockets e Java RMI). Justifique.

   a. [0,5v] Servidor foi reiniciado, tendo obtido um porto diferente desta vez; clientes lançados depois do servidor reiniciar deixam de conseguir invocar a função remota.

   b. [0,5v] É instanciado um proxy do lado do cliente quando a referência remota é estabelecida.

4. Considere o nome "sd.tecnico.ulisboa.pt/exemplo".
   a. [0,4v] Para este nome ser resolvido, é necessário contactar diferentes serviços de nomes. Enumere-os, indicando a porção do nome que é fornecida a cada serviço de nomes e o resultado devolvido por esse serviço de nomes.

   b. [0,4v] Classifique este nome quanto à pureza e homogeneidade.

Grupo III [3,5 valores]

Pretende-se construir um sistema de informação para a receção de medições de temperatura recolhidas por sensores. Estes sensores estão distribuídos por diversos locais e cada sensor está ligado à Internet. Para a concretização do serviço, optou-se pela utilização da tecnologia de Web Services com *binding* para SOAP/HTTP.

1) Utilize a linguagem de programação **Java** com a biblioteca JAX-WS para desenvolver o Web Service seguindo a abordagem *implementation-first*.

   a) [0,5v] Defina uma **classe de dados** que represente uma medição de temperatura, que inclua como atributos o valor medido, assim como a unidade e a marca temporal respetivas.

```
public class MediçãoTemperatura {
```

   b) [0,5v] Defina uma **interface** para o serviço contendo a operação **`receberDados`**(), que recebe uma medição e devolve uma confirmação com a marca temporal no servidor.
   Acrescente tudo o que for necessário para que a interface possa depois gerar um Web Service.

   c) [0,5v] *"Um Web Service desenvolvido com a abordagem implementation-first não usa WSDL."*
   Concorda com a afirmação? Justifique.

Sim/não

d) [0,5v] Qual é o formato de representação dos dados que passa na rede quando existe uma invocação da operação **`receberDados`**()? Indique o nome do formato e esclareça se é um formato de codificação implícita ou explícita, justificando.

2) O endereço do Web Service de medições de temperatura é: http://iotcloud.com:8080/input

a) [0,5v] Como classifica o nome acima quanto ao âmbito? Justifique.

b) [0,5v] *"A utilização do UDDI para registo de Web Services torna o DNS desnecessário"*. Concorda com a afirmação? Justifique.

Sim/não

c) [0,5v] Faz sentido fazer *caching* dos registos de serviços no UDDI num cliente de Web Services? Indique uma vantagem e uma desvantagem, justificando.

Vantagem:
Desvantagem:

Grupo IV [3,5v]

1. Considere um sistema que usa replicação ativa com o protocolo *quorum consensus* estudado nas aulas, constituído por 5 réplicas. Todas as réplicas têm o mesmo peso na votação.
   Os clientes deste sistema encontram-se todos na mesma rede local; cada réplica encontra-se em redes remotas, a diferentes distâncias da rede onde residem os clientes. Mais precisamente, o tempo médio de propagação de uma mensagem entre um cliente e uma réplica (ou vice-versa) é:
   - Réplica 1: 4 ms
   - Réplica 2: 4 ms
   - Réplica 3: 10 ms
   - Réplica 4: 20 ms
   - Réplica 5: 50 ms

   Nas alíneas seguintes, assuma que o tempo que cada réplica demora a executar os pedidos que recebe é aproximadamente nulo. Assuma também que não se perdem mensagens.

a) [0,6v] Assumindo uma situação em que todas as réplicas estão disponíveis e têm todas o valor mais recente, qual o tempo médio que um cliente tem de esperar para ler o valor replicado por este sistema? Justifique.

b) [0,6v] O que mudaria na sua resposta à alínea anterior se a réplica 1 tiver um valor desatualizado em relação às restantes réplicas? Justifique.

c) [0,6v] O que mudaria na sua resposta à alínea a) se o cliente pretender escrever (em vez de ler)? Justifique.

2. Considere agora um sistema que usa replicação passiva, constituído por dois servidores (a cada momento, um é primário, outro é secundário). Os clientes deste sistema invocam procedimentos remotos e esperam pela respetiva resposta. No caso de expirar um temporizador no cliente antes da resposta chegar, o cliente re-envia o pedido para o servidor que é primário nesse momento.
   Assuma que:
   - Cada servidor tem uma *thread* única que trata um pedido remoto de cada vez, por ordem de chegada, demorando $t_{service}$=10s por cada pedido
   - O período de envio de provas de vida (P) é P=30s
   - A comunicação é fiável, e o tempo de transmissão máximo é limitado, garantindo que qualquer mensagem enviada é entregue no máximo ao fim de t_{max}=2s
   - Os servidores falham silenciosamente
   - Um servidor que se torne primário demora, em média, 1h até falhar silenciosamente
   - Em qualquer momento, pelo menos um dos servidores está disponível e tem o estado correto

   a) [0,6v] Na ausência de falhas e no caso em que apenas um cliente está a usar o sistema, qual o tempo máximo de execução do procedimento remoto (tempo desde que cliente enviou pedido até receber a resposta)? Justifique.

   b) [0,6v] Continuando a assumir o cenário de um cliente apenas mas em que um dos servidores pode falhar, qual o tempo máximo de execução do procedimento remoto? Justifique.

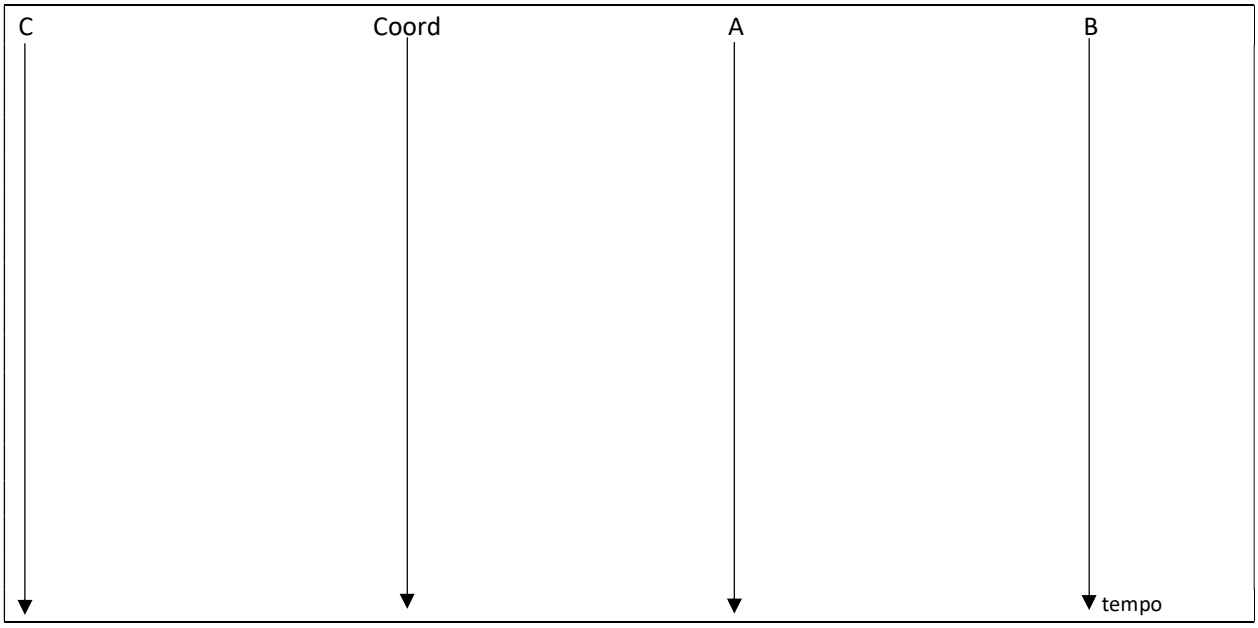
   c) [0,5v] Qual a fiabilidade deste sistema? Justifique.

Grupo V [1,5v]

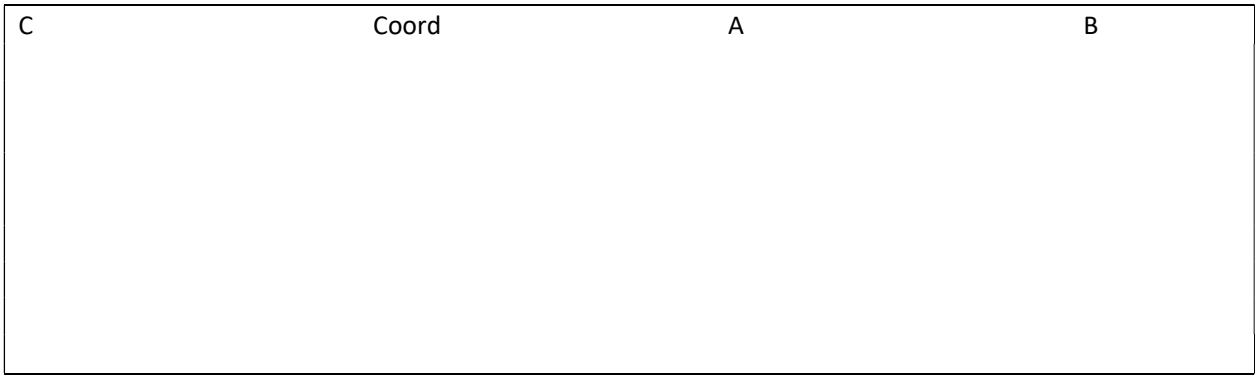
Considere o seguinte programa que invoca procedimentos (LerSaldo e AtualizarSaldo) em servidores remotos distintos (servidor do Banco A e servidor do Banco B) no âmbito de uma transação distribuída. O protocolo de confirmação atómica usado é o 2-Phase Commit.

```
transferência (BancoA, BancoB, Valor) {
1    idDtx = begin_transaction;
2    LerSaldo (BancoA, SaldoA, idDtx);
3    LerSaldo (BancoB, SaldoB, idDtx);
4    AtualizarSaldo (bancoA, saldoA-Valor, idDtx);
5    AtualizarSaldo (bancoB, saldoB+Valor, idDtx);
6    close_transaction(idDtx);
}
```

1. [0,8v] Assuma uma execução sem qualquer falha, em que a transação distribuída é concluída com sucesso. Indique as mensagens trocadas através da rede entre o cliente C, servidor A, servidor B e coordenador Coord (desde a linha 1 à linha 6).



2. [0,7v] Finalmente, assuma uma execução em que a transferência se executa com sucesso até à linha *close_transaction*. No entanto, imediatamente antes do cliente executar essa linha, o servidor B falha permanentemente. Indique as mensagens que são trocadas através da rede entre o cliente C, servidor A, servidor B e coordenador Coord quando a linha *close_transaction* é executada.



Grupo VI [5 valores]

1) [0,5v] Qual é a diferença entre a cifra simétrica e a cifra assimétrica?

2) [0,5v] *"A função de resumo SHA-2 permite cifrar mensagens de forma eficiente."*
Concorda com a afirmação? Justifique.

3) Pretende-se agora criar um sistema de **autenticação** para clientes e servidores de Web Services usando criptografia RSA e o protocolo de transporte HTTP. Assuma que o cliente apenas conhece a sua chave privada, K_{priv_C}, e a chave pública do servidor K_{pub_S}; e vice-versa.

   a) [0,8v] Pretende-se proteger uma mensagem SOAP para garantir a sua autenticidade e integridade. Descreva abaixo qual o conteúdo da mensagem protegida. Proponha uma solução eficiente.

```
<soap:envelope>
    <soap:header>




    <soap:body>
```

   b) [0,5v] *"Para garantir a frescura da mensagem SOAP basta acrescentar um cabeçalho com uma marca temporal."* Concorda com a afirmação? Justifique.

Concordo / não concordo

4) Um cliente autenticou-se no Kerberos na rede do Técnico e recebeu o respetivo ticket TGT e uma chave de sessão. Pretende-se agora usar o serviço S_{salas} de reserva de sala para estudo que pertence ao domínio do Técnico.
   a) [0,5v] Qual é o passo seguinte que o cliente deve efetuar?

   b) [0,5v] Que componente da arquitetura Kerberos permite garantir que apenas alunos do Técnico podem usar o serviço de reserva de salas? Justifique.

   c) [0,5v] Como pode o cliente ter a certeza que está a interagir com o verdadeiro Kerberos e não com um impostor? Justifique.

5) Recomendaria para uso pelo Kerberos os seguintes algoritmos de cifra:
   a) [0,4v] Protocolo RSA com chaves de 2048 bits? Justifique.

   b) [0,4v] Protocolo DES com chaves de 56 bits em modo CBC? Justifique.

   c) [0,4v] Protocolo AES com chaves de 128 bits em modo ECB? Justifique.