LETI/LEIC 2015-2016, Exame de Época Especial de Sistemas Distribuídos

20 julho de 2016

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

Grupo I [3 valores]

```
import java.rmi.*;
public interface BankAccount extends Remote {
        public boolean deposit(float amount) throws RemoteException;
        public boolean withdraw(float amount) throws
          OverdrawnException, RemoteException;
        public String getBalance() throws RemoteException;
}
```

1) [0,5] Considere a interface acima. Procure escrevê-la na IDL do SUN-RPC, inclua todos os elementos que achar necessários propondo os que não conseguir obter diretamente da interface acima. Não se preocupe nesta fase com as exceções.

2) [0,3] A interface em Sun-RPC é semelhante ao código C que é frequente aparecer em ficheiros ".h". Contudo na alínea anterior deverá ter usado aspetos que diferenciam a interface em Sun-RPC de um interface em C. **Indique 2 aspetos** e explique a razão.

3) [0,3] Considerando agora as exceções do método `withdraw()`. Que solução deveria adotar para conseguir que o cliente deste procedimento em Sun-RPC tivesse a mesma informação que tem o método remoto em Java. Apresente a estrutura de dados respetiva.

4) As mensagens de Sun-RPC vão transmitir os dados de forma a garantir que estes sejam corretamente utilizados em qualquer tipo de máquina.
   a) [0,2] Explique a razão deste problema ilustrando com um exemplo da interface.

   b) [0,3] Que tipo de políticas usa o protocolo do Sun-RPC para solucionar o problema da alínea anterior? Justifique.

5) [0,4] Considerando as operações cuja interface se encontra acima, quais consideraria como sendo idempotentes? Justifique.

6) [0,4] Que outra semântica de invocação, habituais nos RPC, teria de ser usada para as outras operações? Justifique.

7) Suponha que se pretende utilizar como protocolo de transporte o UDP. Indique claramente que mecanismos seriam necessários para conseguir esta semântica.
   a) [0,3] No cliente.

   b) [0,3] No servidor.

Grupo II [3,4 valores]

Considere o excerto de um programa Java RMI que procura criar um sistema muito simples de leilões. Para tornar mais claro o programa e concretizar a topologia em que o mesmo está a ser usado considere a Figura 1 que deve ter em conta nas respostas seguintes.

```
import java.rmi.*;
import java.rmi.server.UnicastRemoteObject;

public interface Bid extends Serializable {
      int getAmount();
      int getBidderID();
}
public class BidImpl implements Bid { ... }

public interface BidListener extends Remote {
      void tellMeABid(Bid newBid) throws RemoteException;
}
public class BidListenerImpl implements BidListener { ... }

// Runs an auction, informing all listeners of all bids.
public interface Auction extends Remote {
      void registerBL(BidListener bl) throws RemoteException;
      void makeBid(Bid newBid) throws RemoteException;
}

public class AuctionI extends UnicastRemoteObject implements Auction {
      public void registerBL(BidListener bl) throws RemoteException
// add bl to a collection bls }
      public void makeBid(Bid newBid) throws RemoteException {
// for each bl in collection bls ...bl.tellMeABid(newBid);
}
```

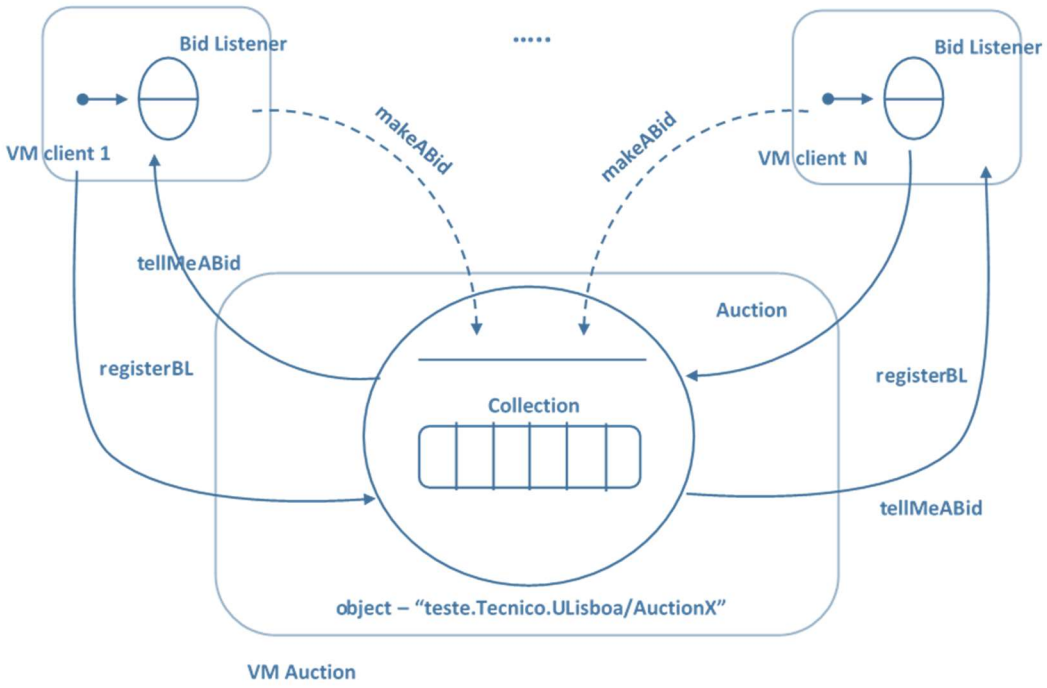


Figura 1

1) Suponha que o cliente no seu programa executa o seguinte conjunto de instruções

```
blClient1 = new BidListenerImpl();
auction.registerBl(blClient1);
```

a) [0,5] Para conseguir executar estas instruções o que necessita o cliente de fazer anteriormente? Programe o que achar necessário.

b) [0,5] Suponha que este cliente quer fazer um novo lance no leilão. Programe como o faria.

2) O Client1 efetuou new do objeto BidListenerImpl

a) [0,4] Explique que operações são executadas pelo RMI quando é efetuado o registo no objeto Auction.

b) [0,4] Quando Auction invoca tellMeABid poderiam existir diversos clientes registados. De que forma é que o objeto Auction consegue ter o contexto de comunicação para aceder as máquinas e sockets corretos? Justifique claramente.

c) [0,4] O método tellMeABID tem como parâmetro newBid. Explique como é efetuada a transferência deste parâmetro e porquê.

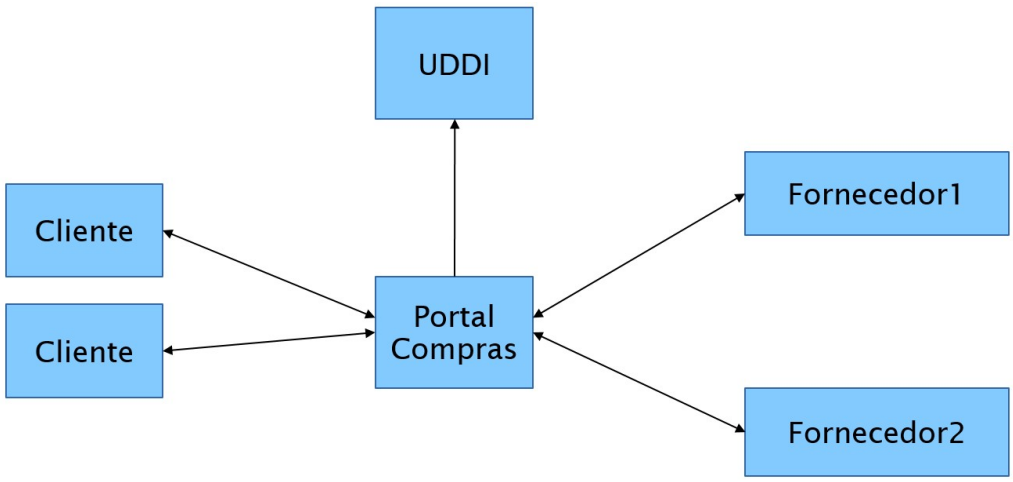
3) Considere que registerBL foi invocado já 6 vezes e makeBid 10.
   a) [0,4] Quantos proxies estão presentes na JVM de auction?

   b) [0,4] Quantos proxies na VM Cliente 1?

4) [0,4] O Client1 termina mas não a JVM onde se executa. O que sucede ao objeto BLClient1? Justifique.

Grupo III [3,4 valores]

Considere o seguinte sistema distribuído, baseado na tecnologia de Web Services. O portal de compras atende múltiplos clientes e efetua vendas *on-line*. O portal encaminha as pesquisas recebidas dos clientes para os seus fornecedores. Depois, agrega as respostas, e responde ao cliente.



1) [0,4] Que frase melhor descreve a função do WSDL nos Web Services?
   A. Descrição da interface abstrata do serviço.
   B. Formato canónico para a representação dos tipos de dados como datas e numéricos.
   C. Descrição da interface das operações do serviço e respetiva concretização.
   D. Protocolo de transporte das mensagens de pedido e resposta.

2) [0,5] Considere novamente a figura. Quantos WSDL deveriam existir para suportar todas as interações que são ilustradas? Justifique.

3) [0,6] Qual é a formatação das mensagens enviadas por um Cliente ao Portal de Compras? Indique uma vantagem e uma desvantagem do formato utilizado, justificando.

4) [0,7] Qual é a função dos stubs num cliente de Web Services? Explique detalhadamente.

5) Suponha agora que existem os seguintes objetos capazes de intercetar mensagens de Web Services.
   - *LogHead* - imprime os cabeçalhos da mensagem para a consola
   - *LogBody* - imprime o corpo da mensagem para a consola
   - *ZipBody* - aplica o algoritmo de compressão/descompressão ZIP ao corpo da mensagem.

   Considere a seguinte configuração de cadeias de intercetores:
   - Cliente: *ZipBody*
   - Servidor: *LogHead, ZipBody, LogHead*

   a) [0,4] Quando é feita a invocação remota de uma operação do WS, qual é a sequência de execução do pedido desde o **cliente** até que o **servidor** receba e execute o pedido?
      A. Cliente, Stub, ZipBody, Rede, LogHead, ZipBody, LogHead, Tie, Servidor
      B. Cliente, ZipBody, Stub, Rede, Tie, LogHead, ZipBody, LogHead, Servidor
      C. Cliente, ZipBody, Stub, Rede, Tie, LogHead, ZipBody, Servidor
      D. Cliente, ZipBody, Rede, LogHead, ZipBody, LogHead, Servidor

   b) [0,4] É possível ao Servidor acrescentar `LogBody` à sua *handler chain* sem recompilar/reconfigurar o Cliente? Porquê?

   c) [0,4] O que acontece na invocação remota se o `ZipBody` no servidor intercetar uma mensagem à chegada (*inbound*) e, por algum motivo, lançar uma exceção `java.lang.RuntimeException`?

Grupo IV [4 valores]

1) Considere novamente o sistema distribuído do Grupo III, do portal de compras e fornecedores.

   a) Considere que tem à sua disposição apenas **criptografia simétrica**.
   Proponha um esquema de segurança que garanta a **confidencialidade** das mensagens.
   Use a notação { } para representar cifras. Identifique as chaves de forma clara.

      i) [0,3] Distribuição prévia de chaves. Indique que chaves existem e quem as conhece.

      ii) [0,4] Descreva os passos de processamento de mensagem à saída do portal.

      iii) [0,4] Descreva os passos de processamento de mensagem à chegada do fornecedor.

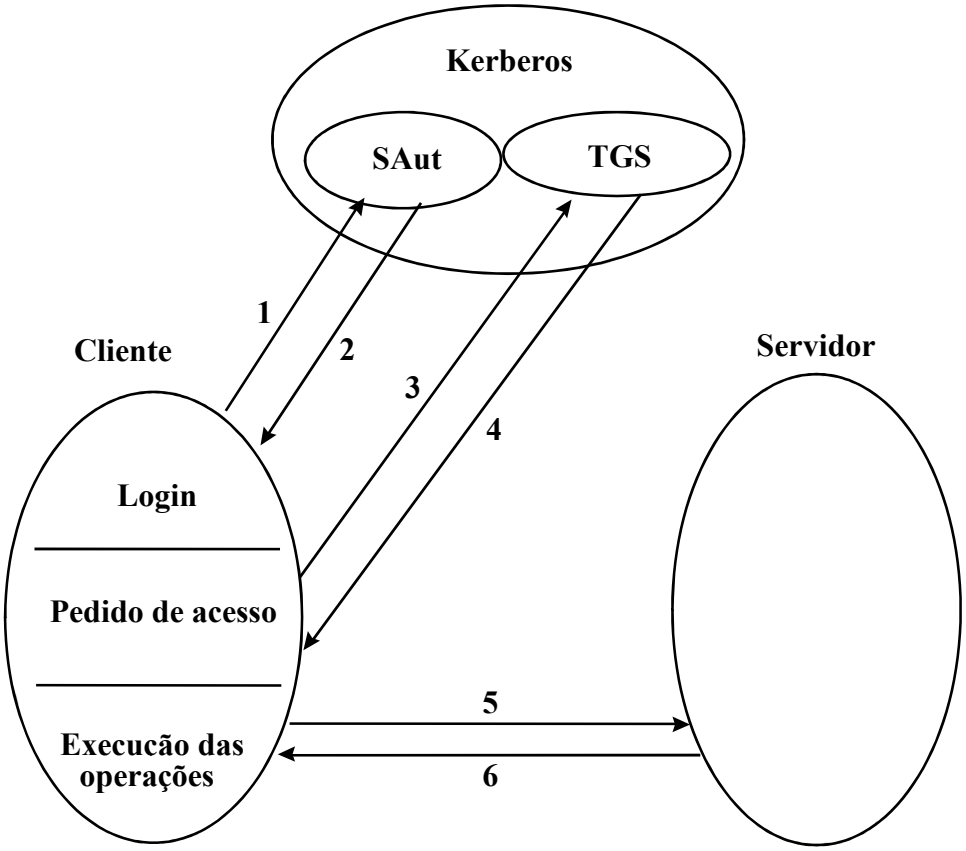
   b) Considere agora que dispõe também de **criptografia assimétrica**.
   Proponha um esquema de segurança que garanta a **confidencialidade** e **autenticidade** das mensagens mas que evite a cifra de grandes volumes de dados com cifra assimétrica.

      i) [0,5] Descreva os passos de processamento de mensagem à saída do portal.

      ii) [0,5] Descreva os passos de processamento de mensagem à chegada do fornecedor.

      iii) [0,4] Considera que a sua solução é segura face a ataques por repetição?
      Indique o que previne os ataques ou o que mudaria para os prevenir.

2) Considere um sistema Kerberos V5 resumido na figura seguinte.



a) [0,4] Qual é a distribuição de chaves que deve ter sido feita antes de se iniciar o protocolo?
   A. Cliente e Servidor devem ter partilhado uma chave simétrica entre si.
   B. SAut deve ter a chave simétrica do Cliente, TGS deve ter a chave simétrica do Servidor.
   C. SAut deve ter a chave pública do Cliente, TGS deve ter a chave pública do Servidor.
   D. SAut deve conter certificados digitais de todas as entidades do sistema, assinados por uma CA.

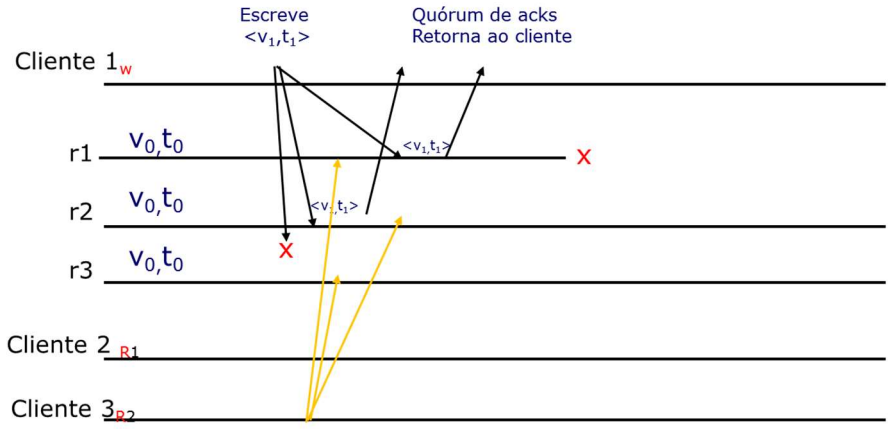
b) [0,3] Como pode o cliente saber que se autenticou perante o verdadeiro SAut e não um impostor?

c) [0,4] Qual é a sua função do TGS? Descreva referindo-se aos passos do protocolo identificados na figura.

d) [0,4] Indique 3 elementos que devem constar de um Ticket Kerberos.
   Descreva sucintamente a utilização que o protocolo dá a cada elemento que indicar.

Grupo V [3,1 valores]

1) Considere o seguinte diagrama de um protocolo de quóruns de maioria com 3 réplicas ativas. As setas representam mensagens enviadas.



a) [0,3] O que são os valores <vi, ti> ?

vi
ti

b) [0,4] Que valor vai ser lido pelo Cliente 3? Justifique.

c) [0,3] Quantas faltas tolera o sistema da figura? Justifique.

d) [0,4] Quantas réplicas seriam necessárias para tolerar 5 faltas? Justifique.

2) Considere um sistema replicado, baseado no protocolo ***primary-backup***, tendo em conta que não existe servidor de nomes.
Legenda: C – cliente; FE - ?; S – serviço; R1 – réplica primária; R2 – réplica secundária; x variável inteira.

Registaram-se as seguintes mensagens:

- C -> FE write(x, 10)
- R1 -> R2 I'm alive
- FE -> R1 write (x, 10)

a) [0,2] O que é o componente FE? Qual é a sua função?

b) [0,4] O que deve R1 fazer depois de receber o write(x, 10) ?

c) [0,3] Descreva uma situação de falta silenciosa neste protocolo. Justifique a sua resposta.

d) [0,3] Das seguintes situações, escolha a que corresponde a uma falta bizantina:
   A. R1 pára de responder a pedidos e deixa de enviar I'm Alives.
   B. R1 pára de responder a pedidos e continua a enviar I'm Alives.
   C. R1 fica mais lento mas continua a enviar I'm Alives.
   D. Nenhuma das anteriores.

e) [0,5] Considere que a escrita foi feita até ao fim e que outro cliente pretende agora executar ***read(x)***.
Complete a sequência até que o cliente 2 receba uma resposta (caso receba).
R1 KO representa a falta silenciosa de R1. Se necessário acrescente mais ● à sua resposta.

- C2 -> FE2 read (a)
- FE2 -> R1 read (a)
- **R1 KO**
-
-
-
-
-

-
-
-
-
-
-

Grupo VI [1,6 valores]

Considere o seguinte cenário de utilização. Um cliente pretende executar o seguinte programa que interage com 3 servidores RM1, RM2, RM3:

① Ler as variáveis x e y em RM1;

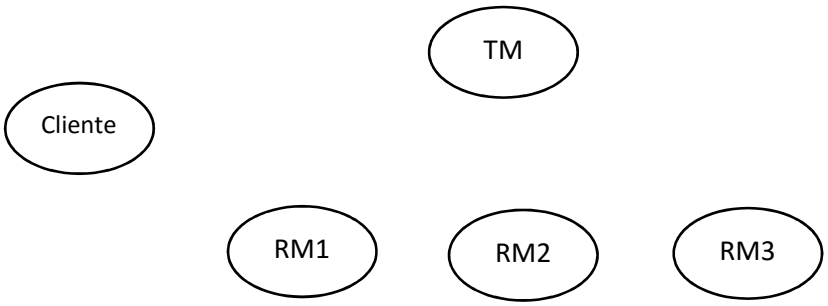
② Escrever o valor x/y no servidor RM2

③ Escrever o valor y/x no servidor RM3.

Pretende que toda a operação respeite as propriedades ACID e que os valores escritos não sejam exceções matemáticas.

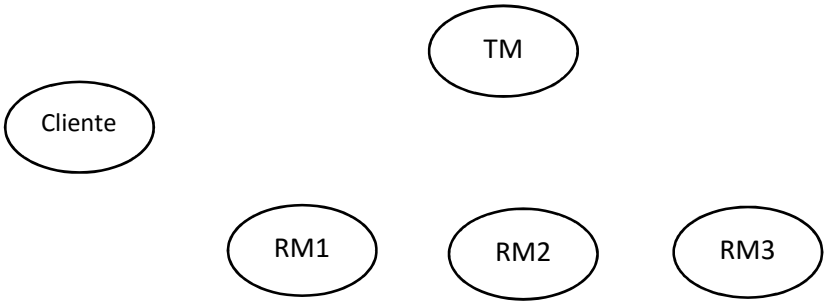
1) [0,5] Escreva o código do cliente incluindo todos os elementos que achar necessários para executar o programa. Considere que existem as operações read e write nos servidores.

2) [0,4] Considere o seguinte diagrama relativo ao programa anterior:



Complete incluindo todas as mensagens representadas por setas com legenda até o programa ter terminado a etapa ②.

3) [0,4] Complete o diagrama desde o momento em que o cliente despoleta o protocolo de 2PC e até uma decisão ser tomada.



4) [0,3] Considere na situação da alínea anterior que a ligação a RM3 está anormalmente lenta e este respondeu ao TM depois de expirar o time-out desta fase.
O que pode ocorrer? Se considerar que há várias hipóteses, indique-as explicando-as.

Grupo VII [1,5 valores]

1) [0,2] Porque é que os nomes puros são mais difíceis de usar
   A. Porque não são hierárquicos.
   B. Porque não tendo informação de localização não permite orientar o algoritmo de resolução.
   C. Porque são mais difíceis de criar.
   D. Porque são normalmente binários e não podem ser usados em XML.

2) [0,2] Nomes hierárquicos:
   A. Permitem assegurar unicidade referencial mais facilmente em redes de grande escala.
   B. São necessariamente homogéneos.
   C. São necessariamente de âmbito global.
   D. Todas as anteriores.

3) Considere novamente o sistema do Grupo III, Portal de Compras.
Todos os componentes representados na figura comunicam com o UDDI, apesar de na figura apenas estar representada uma interrogação do Portal de Compras ao UDDI.

a) [0,4] O que motiva o Portal de Compras a interrogar o UDDI?
Dê um exemplo indicando os argumentos da interrogação e uma possível resposta.

b) [0,4] Que mais informação pode ser guardada num registo UDDI?
Dê dois exemplos e explique sucintamente a utilidade da informação referida.

c) [0,3] Um conceito inovador do UDDI é poder classificar os atributos dos objetos com taxonomias predefinidas. Explique o conceito e indique uma taxonomia que faria sentido utilizar.
