LEIC 2018/19, 1º Exame de Sistemas Distribuídos

18 de junho de 2019

Identifique todas as folhas. Responda no enunciado, usando apenas o espaço fornecido.

Nas perguntas de escolha múltipla existe apenas uma resposta certa. Em caso de dúvida, pode selecionar uma ou mais alíneas. A nota é calculada pelas alíneas que escolheu na sua resposta, da seguinte forma: a alínea correta conta com a cotação completa; cada alínea incorreta desconta 1/3 da cotação da pergunta.

Duração da prova: **2h00m**

Grupo I – RPC [3,5 valores]

1) Considere um RPC genérico que comunica usando o protocolo **UDP** e que implementa a seguinte operação:

```
// acrescenta uma linha no final de um ficheiro de log (registo de atividades)
void WRITE_LOG_ENTRY(string);
```

O RPC dispõe das seguintes opções globais de configuração (aplicam-se aos clientes e aos servidores):

```
timeout = 500ms;
retry = true;
addRequestIdentifiers = false;
keepResponseHistory = false;
```

a) [0,6v] A operação é idempotente? Justifique.

b) [0,6v] Qual é a semântica de invocação garantida pela configuração acima? Justifique.

c) [0,7v] Ajuste a configuração de modo a que a semântica da operação WRITE_LOG_ENTRY seja o mais idêntica possível à de uma operação local. Justifique cada uma das opções de configuração modificadas.

O mais próximo que se consegue com as opções indicadas é a semântica no-máximo-uma-vez.

addRequestIdentifiers = true; // para que cada mensagem possa ser identificada de forma única

// e deste modo o servidor possa reconhecer e não executar mensagens retransmitidas

keepResponseHistory = true; // para que o servidor memorize as respostas e possa devolver

// novamente a mesma resposta para um pedido retransmitido

2) Considere a seguinte definição na linguagem **protobuf** (*Protocol Buffers*) usada no **gRPC**:

```
message Product {
  string identifier = 1;
  string description = 2;
  int32 quantity = 3;
}
message ProductsRequest {
}
message ProductsResponse {
  string supplierIdentifier = 1;
  repeated Product product = 2;
}
service Supplier {
  rpc listProducts(ProductsRequest) returns (ProductsResponse);
}
```

a) [0,5v] O *protobuf* resolve o problema da heterogeneidade da representação de tipos de dados entre diferentes linguagens de programação? Justifique.

b) [0,7v] Defina em **protobuf** a operação `orderProduct` que recebe um identificador de produto e uma quantidade, e depois devolve um identificador de encomenda.

c) [0,4v] Defina em **Java** a assinatura do método que será gerado pela ferramenta **protoc** a partir da definição da alínea anterior e deverá depois ser implementada no servidor.

```
public void orderProduct(ProductRequest request, StreamObserver<ProductResponse>
responseObserver);
```

Grupo II – RMI [3 valores]

Considere a aplicação móvel de uma cadeia internacional de restaurantes, baseada em Java RMI. A aplicação permite aos clientes habituais consultarem qual o restaurante mais perto de si e, caso pretendam, reservarem mesa nesse restaurante.

Considere os seguintes excertos de duas interfaces Java deste sistema.

```
public interface IRestaurantBrowser extends Remote {
    // retorna o restaurante que está mais próximo das coordenadas passadas por argumento
    IRestaurant findNearestRestaurant(float latitude, float longitude)
        throws RemoteException;
    ...
}

public interface IRestaurant extends Remote {
    // tenta reservar uma mesa no restaurante
    Reservation reserve(String clientName, int numPersons, DateTime when)
        throws RemoteException, ReservationNotPossible;
    ...
}

public class Reservation implements Serializable {
    ...
}
```

Existe uma instância de IRestaurantBrowser a correr num servidor e registada num RMI Registry com o nome "//xpto.restaurants.com/rstbrowser".

1) [1,2v] Programe um método Java que tenta reservar mesa para um conjunto de pessoas no restaurante mais próximo. O método recebe todos argumentos necessários: coordenadas atuais, nome do cliente, número de pessoas, data e hora da reserva. O método deve retornar um objeto do tipo Reservation caso a reserva tenha sucesso ou null caso contrário. Na sua resposta, pode omitir a configuração do SecurityManager. Não se esqueça de tratar eventuais erros da invocação remota.

```
public Reservation reserveTableAtNearestRestaurant(
(float lat, float lon, String clientName, int numPersons, DateTime when) {









}
```

2) [0,6v] Quantas referências remotas são criadas pelo método acima quando este é executado sem erros?
   A. Nenhuma
   B. Uma
   C. Duas
   D. Três ou mais

   C

3) [0,6v] Sabendo que o Java RMI usa o método de contagem de referências para gerir a recolha automática de memória (*garbage collection*) dos objetos remotos, indique quantas vezes a operação addRef é chamada de cada vez que o método *reserveTableAtNearestRestaurant* se executa com sucesso.

A. Nenhuma
B. Uma vez
C. Duas vezes
D. Três ou mais

C

4) [0,6v] O tipo Reservation corresponde a uma classe Java que não herda de Remote e que implementa a interface Serializable. Quando o cliente chama o método *reserve* e recebe o seu retorno, qual classe é instanciada do lado do cliente?

A. A classe proxy de Reservation.
B. A classe Reservation, sempre.
C. A classe do objeto efetivamente retornado, que pode ser Reservation ou uma sub-classe desta.
D. Nenhuma classe é instanciada.

C

Grupo III – Web Services [3,5 valores]

Considere o seguinte documento **WSDL** que define um serviço de **validação de cartão de crédito (CC)**.
O documento tem algumas omissões assinaladas com "...".

```
<definitions ...
      targetNamespace="http://ws.sdis.tecnico.ulisboa.pt/"
      name="CreditCardImplService">
      <types>
            <xsd:schema>
               ...
            </xsd:schema>
      </types>
      <message name="validateNumber">
            <part name="parameters" element="tns:validateNumber"/>
      </message>
      <message name="validateNumberResponse">
            <part name="parameters" element="tns:validateNumberResponse"/>
      </message>
      <portType name="CreditCard">
            <operation name="validateNumber">
                  <input message="tns:validateNumber"/>
                  <output message="tns:validateNumberResponse"/>
            </operation>
      </portType>
      <binding name="CreditCardImplPortBinding" type="tns:CreditCard">
            <soap:binding transport="http://schemas.xmlsoap.org/soap/http"
                        style="document"/>
            <operation name="validateNumber">
                  ...
            </operation>
      </binding>
      <service name="CreditCardImplService">
            <port name="CreditCardImplPort" binding="tns:CreditCardImplPortBinding">
                  <soap:address location="http://sd.rnl.tecnico.ulisboa.pt:8080/cc"/>
            </port>
      </service>
</definitions>
```

1) [0,6v] Para este serviço em concreto, o que deveria estar definido na secção `xsd:schema`?
   Nota: explique por palavras, não necessita de usar a sintaxe xsd.

A secção *schema* deveria conter a definição dos tipos de dados que são depois utilizados pelas mensagens do Web Service. Neste caso concreto, deveriam ter a definição dos argumentos da operação (número de cartão de crédito) e o resultado (booleano).

2) [0,5v] Suponha que, em vez de utilizar para protocolo de transporte o HTTP, pretende usar SMTP. Em que secção do WSDL deveria especificar esta alteração?
   A. `message`
   B. `portType`
   C. `binding`
   D. `port`

   C

3) [0,8v] Escreva uma mensagem **SOAP** correspondente ao **pedido** de validação do número 4024007102923925. Pode omitir as definições de espaços de nomes *xmlns*.

4) [0,5v] Qual é o elemento definido dentro do SOAP para devolver informação de que a operação remota não teve sucesso e lançou uma exceção?
   A. `<Handler>`
   B. `<Fault>`
   C. `<Error>`
   D. `<Failure>`

   B

5) [0,6v] O elemento `port` contém o endereço de invocação do serviço (definido no atributo `location` do elemento `soap:address`). Esse endereço é um nome puro ou impuro? Justifique.

O URL é um nome impuro. É constituído por diversas partes – protocolo, nome de domínio DNS, porto e caminho - em que cada uma das partes é usada por um dos passos de resolução. Se o objeto mudar de localização, o nome deixa de o referenciar.

6) [0,5v] Qual dos seguintes itens de informação NÃO pode ser guardado no UDDI?
   A. Referência remota para objeto Java
   B. URL do serviço
   C. Morada da organização
   D. Classificação da área de negócio do serviço

   A

Grupo IV – Tolerância a Faltas [4 valores]

Considere um sistema replicado usando o protocolo Quorum Consensus (QC) ensinado nas aulas teóricas. Este sistema tem 3 réplicas, todas valendo o mesmo peso, e usa quóruns de maioria para ler e escrever. Num dado instante, o estado das réplicas é o seguinte:

R1: <val = 10, <seq-no: 5, cli-id: 1>>
R2: <val = 10, <seq-no: 5, cli-id: 1>>
R3: <val = 20, <seq-no: 6, cli-id: 2>>

1) [0,8v] Se um cliente iniciar uma leitura no estado acima, que valor observará?
   A. 10
   B. 20
   C. 10 ou 20, depende das respostas que receber primeiro
   D. A leitura não poderá completar enquanto o estado não evoluir.

   C

2) [0,8v] Considere a escrita do valor 20 com *tag* <seq-no: 6, cli-id: 2>. Qual das afirmações seguintes é verdadeira?
   A. A escrita já foi completada com sucesso.
   B. A escrita já foi completada mas sem sucesso.
   C. A escrita ainda está em curso.
   D. Nenhuma das anteriores.

   C

3) [1,2v] Assuma que, durante um dado período, a latência de rede (em ambos os sentidos) entre um *front-end* FE1 e cada gestor de réplica é exatamente: **10 ms** entre FE1 e R1; **50 ms** entre FE1 e R2; **100 ms** entre FE1 e R3.

   Assuma também que:
   - 90% das operações executadas por FE1 são leituras e os restantes 10% são escritas;
   - o tempo de processamento local é negligenciável;
   - no período em causa, nenhuma réplica falha.

   Compare o desempenho do QC com quóruns de maioria – **alternativa A** – com uma variante em que RT=1 e WT=3 (RT: *read threshold*, WT: *write threshold*) – **alternativa B**.
   Na sua resposta, comece por indicar qual a alternativa em que, globalmente, FE1 obtém melhor desempenho. De seguida justifique a sua resposta quantificando, para cada alternativa, o tempo médio de acesso ao sistema por parte de FE1. Respostas sem justificação não serão cotadas.

   Alternativa mais rápida:

   Alternativa B

   Justificação (calcular tempo médio de acesso):

   Alternativa A:
   tLer(A) = 2 x max(10,50) = 100 ms tEscrever(A)=tLer(A) + 2 x max(10,50) = 200 ms
   tMedio(A) = 90% x tLer(A) + 10% x tEscrever(A) = 90+20 = 110 ms

   Alternativa B:
   tLer(B) = 2 x 10 = 20 ms tEscrever(B)=tLer(B) + 2 x max(10,50,100) = 220 ms
   tMedio(B) = 90% x tLer(B) + 10% x tEscrever(B) = 18+22 = 40 ms

   (também se considerou correta a interpretação de que a latência indicada no enunciado era relativa ao tempo de envio+receção de mensagem.)

4) Considere agora uma outra variante do QC em que RT=1 e WT=1.
   a) [0,5v] Considerando o teorema CAP, quais propriedades são asseguradas por esta solução?
      A. Consistência forte e Disponibilidade
      B. Consistência forte e Tolerância a partições
      C. Disponibilidade e Tolerância a partições
      D. Consistência forte, Disponibilidade e Tolerância a partições

      C

   b) [0,7v] Esta solução assegura a garantia de consistência sequencial? Se sim, justifique. Se não, apresente um contra-exemplo simples em que 1 ou 2 clientes executam uma sequência de leituras/escritas sobre o sistema replicado e o que observam não é sequencialmente consistente.

Não garante. Contra-exemplo simples:
- Sistema replicado começa com valor 0 em todas as réplicas
- Cliente C executa escrita de valor 1, que é confirmado pela réplica R1 apenas
- Cliente C executa leitura, que recebe e retorna resposta da réplica R2, ou seja o valor 0

Não há nenhuma serialização correta destas duas operações que respeite a ordem local do cliente C, logo o sistema não garante consistência sequencial.
(muitos outros contra-exemplos poderiam ser apresentados.)

Grupo V – Transações Distribuídas – [1 valor]

1) [0,5v] Considere o seguinte programa de uma transação distribuída com o protocolo 2PC, em que as contas bancárias de destino estão alojadas em servidores remotos.

```
boolean makeTransfer(List<TransferInfo> transfers, Account sourceAccount) {
    Object tx = ...
        for (TransferInfo t : transfers) {
            sourceAccount.transferFrom(t.targetAccount, t.amount, tx);
    }
    return closeTransaction(tx);
}
```

Para que o código acima faça sentido, deve substituir "..." por:

A. `doTransactionVoting();`
B. `beginTransaction();`
C. `voteCommit();`
D. `commitTransaction();`

B

2) [0,5v] Numa transação com 3 participantes, seguindo o protocolo 2PC para confirmar a transação, o Coordenador recebeu voto NÃO do primeiro participante que contactou.
   A. Espera pela maioria dos votos dos participantes em falta e só depois envia *cancelarGlobal* a todos.
   B. Espera pela maioria dos votos dos participantes em falta e só depois envia *confirmarGlobal* a todos.
   C. Escusa de esperar por outros votos; pode enviar imediatamente a ordem de *cancelarGlobal* a todos os participantes.
   D. Escusa de esperar por outros votos; pode enviar imediatamente a ordem de *confirmarGlobal* a todos os participantes.

   C

Grupo VI – Segurança [5 valores]

1) Considere novamente o serviço gRPC definido na pergunta 2 do Grupo I, ou seja, o serviço **`Supplier`**.
O serviço irá ser utilizado para integração de parceiros de negócio que dialogam através da **Internet**.

Pretende-se garantir as propriedades da **autenticidade**, **integridade** e **não repúdio** na resposta da operação `listProducts`. Ignore, para já, a frescura e a distribuição de chaves criptográficas.

a) [0,5v] O que acrescentaria à mensagem de resposta do serviço?

Uma assinatura digital com chave privada exclusiva do servidor e cliente com chave pública.
(o MAC com criptografia simétrica não consegue garantir o não-repúdio)

b) [0,6v] Que passos de processamento deverá realizar do lado do servidor ao produzir a resposta? Nomeie as funções criptográficas concretas que está a usar.

Resume mensagem M com função SHA-256 produzindo resumo H.
Cifra do resumo H com RSA-2048 usando chave privada do emissor, produzindo assinatura S.
Envia M e S para o cliente.

c) [0,6v] Que passos de processamento deverá realizar do lado do cliente ao receber a resposta? Novamente, nomeie as funções criptográficas.

Resume mensagem recebida M' com SHA-256 produzindo resumo H'.
Decifra S com RSA-2048 usando a chave pública do emissor, obtendo H.
Se resumo recalculado H' for igual a resumo decifrado H então a mensagem não foi modificada e
foi garantidamente enviada pelo servidor (uma vez que só ele possuí a chave privada).

2) O serviço **`Supplier`** tem um **certificado digital de chave pública** emitido pela autoridade **VeriSign**.

a) [0,6v] *"A chave pública RSA contida no certificado do servidor permite que qualquer cliente envie mensagens que apenas o servidor consegue ler."* Concorda com a afirmação? Justifique.

b) [0,8v] Indique qual o **conteúdo** e **proteção criptográfica** do certificado. Assuma que o certificado segue o formato X.509 e que foi emitido no dia 22 de julho de 2018. Para os restantes campos escolha valores que lhe pareçam razoáveis. Inclua uma legenda na sua resposta.

Sujeito: Supplier, **Chave pública** 0x013fh227…
Emissor: Verisign
Validade: 22 de julho de 2018 até 21 julho de 2020 (ou outra data de fim)
Versão: 1
Número de série: 1234…
Informação adicional…
Assinatura digital de toda a informação anterior usando cifra assimétrica (e.g. RSA-2048) com a chave privada da Verisign.
O certificado pode depois ser verificado com a chave pública da VeriSign.

3) Assuma que a rede de serviços do IST usa o **Kerberos V5** como sistema de autenticação para os utilizadores e que são disponibilizados os serviços: *Mail*, *Files* e *Print*. Por omissão, a autenticação inicial do utilizador tem a validade de 8 horas e a autorização de acesso a um serviço tem a validade de 1 hora.

a) [0,5v] Que chave deve conhecer a utilizadora alice@tecnico.ulisboa.pt para poder autenticar-se? Quem mais deve conhecer essa chave ?

b) [0,8v] Descreva o **conteúdo** e **proteção criptográfica** de um *ticket* obtido por Alice para aceder ao servidor *Print*. Inclua uma legenda na sua resposta.

c) [0,6v] Em média, quanto tempo demora a revogação de permissões de acesso da utilizadora Alice ao servidor *Print*? Como se pode reduzir esse tempo? Justifique a sua resposta.

A permissão é verificada pelo TGS no momento de emissão do *ticket*.

Em média uma revogação demorará 30 minutos (apanhará o *ticket* a meio do prazo de validade).

Para reduzir este tempo seria necessário o TGS reduzir o tempo de validade do *ticket* na emissão.