LEIC 2018/19, 2º Exame de Sistemas Distribuídos
9 de julho 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 com o protocolo **UDP** e que implementa as seguintes operações com mensagens de **pedido-resposta**:

```
// debita dinheiro numa conta bancária, devolve saldo decrementado
DEBIT (string accountId, integer value) -> (integer balance)

// credita dinheiro numa conta bancária, devolve saldo incrementado
CREDIT (string accountId, integer value) -> (integer balance)
```

Considere que existem duas contas bancárias, A e B, com saldo inicial de 100 e 0, respetivamente.
O cliente vai chamar duas operações: DEBIT(A, 50), CREDIT(B, 50) em **paralelo** e de forma **assíncrona**.

a) [0,7v] Qual é o saldo final das contas nas seguintes situações?

Semântica configurada	**Acontecimentos diferentes do normal**	**Saldo final A**	**Saldo final B**
Talvez	Pedido DEBIT perde-se 1 vez.		
Talvez	Resposta DEBIT perde-se 1 vez.		
Pelo-menos-uma-vez	Pedido DEBIT perde-se 1 vez. Pedido CREDIT perde-se 2 vezes.		
Pelo-menos-uma-vez	Pedido DEBIT perde-se 1 vez. Resposta CREDIT perde-se 2 vezes.		
No-máximo-uma-vez	Resposta DEBIT perde-se 1 vez. Pedido CREDIT perde-se 3 vezes.		
No-máximo-uma-vez	Pedido DEBIT perde-se 2 vezes. Resposta CREDIT perde-se 1 vez.		

b) [0,5v] Qual é a semântica de execução garantida pelo RPC caso se troque o protocolo UDP por **TCP**? Justifique detalhadamente.

2) Considere a seguinte definição na linguagem **protobuf** (*Protocol Buffers*) usada no **gRPC** do jogo do galo (Tic-Tac-Toe):

```
message GetBoardRequest { }
message GetBoardResponse { string board = 1; }

message PlayRequest {
  uint32 row = 1;
  uint32 column = 2;
  uint32 player = 3;
}
message PlayResponse {
  enum PlayResult {
    UNKNOWN = 0;
    OUT_OF_BOUNDS = 1;
    SQUARE_TAKEN = 2;
    WRONG_TURN = 3;
    GAME_FINISHED = 4;
    SUCCESS = 5;
  };
  PlayResult result = 1;
}

message CheckWinnerRequest { }
message CheckWinnerResponse { sint32 result = 1; }

service TTT {
  rpc GetBoard(GetBoardRequest) returns (GetBoardResponse);
  rpc Play(PlayRequest) returns (PlayResponse);
  rpc CheckWinner(CheckWinnerRequest) returns (CheckWinnerResponse);
}
```

a) [0,5v] A ferramenta **protoc** permite gerar código numa linguagem alvo.
Qual das seguintes partes de código NÃO é gerada pela ferramenta?

A. Conversão dos tipos de dados.
B. Publicação e pesquisa de serviços num registo global da Google.
C. Definição de interfaces das operações RPC na linguagem alvo.
D. Gestão do canal de comunicação.

b) [0,5v] Ao passar na rede, qual é o formato dos dados transmitidos por uma chamada gRPC ?

A. Dados codificados em binário.
B. Dados codificados em texto em formato XML.
C. Dados codificados em texto em formato JSON.
D. Dados codificados em texto em formato CSV.

c) [0,7v] Escreva código Java de um cliente que use a biblioteca gRPC para fazer uma jogada na posição 2, 2 do tabuleiro em nome do jogador 1, e que depois imprima o tabuleiro para a consola. Assuma que o servidor está a correr na máquina `svc.sd.pt` no porto `8000`.

d) [0,6v] Considera o nome `svc.sd.pt:8000` global e homogéneo? Justifique.

Global?
Homogéneo?

Grupo II – RMI [3 valores]

Considere um sistema distribuído construído sobre Java RMI no qual diferentes servidores A, B, C, ... mantêm repositórios locais de objetos do tipo XPTO. Mais precisamente, cada servidor tem instanciado um objeto remoto que oferece a seguinte interface:

```
public interface XPTOStore extends Remote {
    XPTO get(int key) throws RemoteException;
    void put(XPTO e, int key) throws RemoteException;
}
```

Assuma também que um objeto do tipo XPTO`Store` mantido por cada servidor foi previamente registado junto do RMI Registry com o nome "`//sd.tecnico.pt/store`" concatenado com o nome do servidor A, B, C, etc.

1) [0,9v] Programe um método Java (de uma qualquer classe cliente) que obtém um objeto do repositório de um dado servidor e o adiciona ao repositório de outro servidor. Na sua resposta, pode omitir a configuração do SecurityManager. Não se esqueça de tratar eventuais erros da invocação remota.

```
public void putAtAnotherServer(int key, char fromServer, char toServer) {









}
```

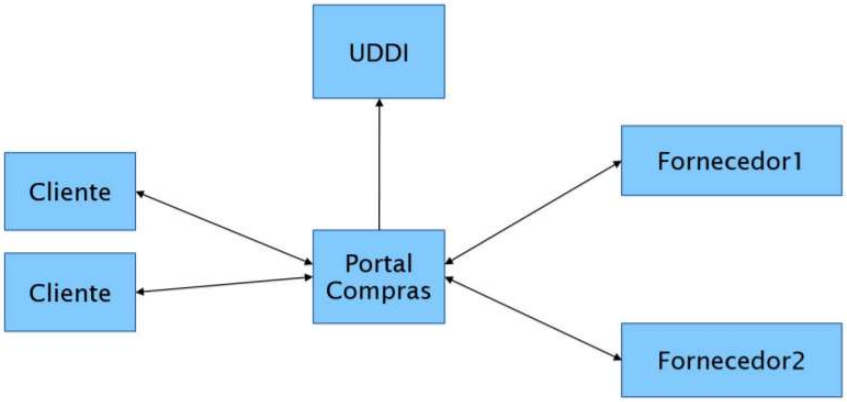
2) [0,8v] Assuma que o tipo XPTO implementa a interface `Remote`.
   Numa execução sem falhas do método `putAtAnotherServer`, quantos objetos *proxy* foram criados durante a sua execução e até ao momento em que o método se prepara para retornar?
   Na sua resposta, para cada *proxy* indique claramente: o processo em que foi instanciado (cliente, fromServer ou toServer), o tipo do *proxy* e o objeto que o *proxy* representa.

3) [0,7v] Considere que o conjunto dos atributos do tipo XPTO é de uma dimensão muito superior àquela de uma referência remota em Java RMI (a título ilustrativo, suponha que os atributos do objeto ocupam 100KBytes e a referência 1KByte).
Se pudesse optar entre o tipo XPTO ser *`Remote`* ou *`Serializable`*, qual opção escolheria para que o método `putAtAnotherServer` fosse mais eficiente do ponto de vista de rede? Justifique.

4) [0,6v] Considerando o nome hierárquico "`//sd.tecnico.pt/storeA`", indique pelo menos 3 autoridades associadas a este nome. Para cada autoridade, indique a componente do nome gerida por essa autoridade.

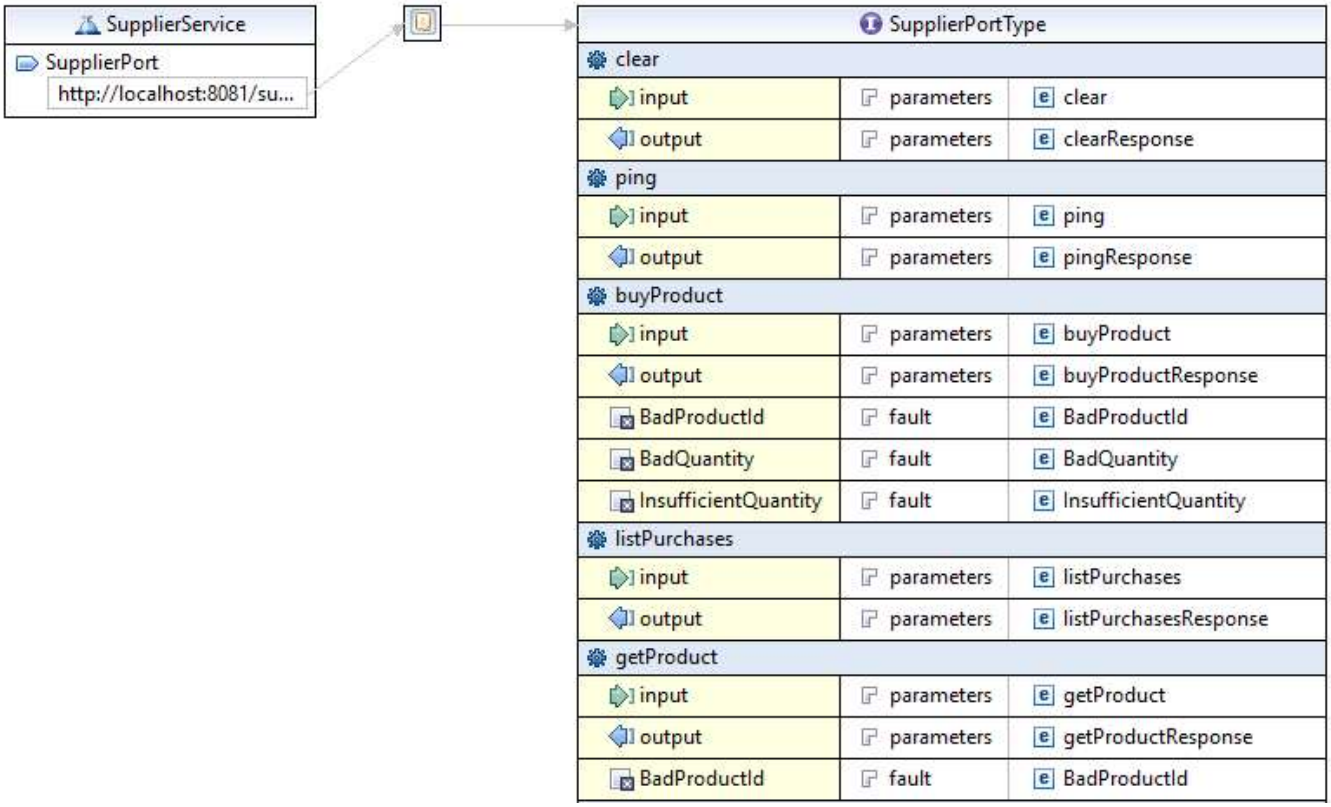
Grupo III – Web Services [3,5 valores]

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.



1) [0,7v] O portal optou por oferecer aos seus clientes apenas uma interface REST. Indique uma vantagem e uma desvantagem desta opção comparando com uma interface SOAP descrita por WSDL. Justifique.

2) Considere a seguinte representação esquemática do WSDL dos fornecedores, produzida pelo ambiente de desenvolvimento Eclipse:



a) [0,6v] O BadProductId:

A. É uma *fault* que pode ser usada pelo serviço para assinalar um erro.
B. É um tipo de dados que define um possível *input* para a operação remota.
C. É um valor enumerado que pode ser devolvido como *output* pela operação remota.
D. É um identificador de operação que depois é utilizado pela função de despacho.

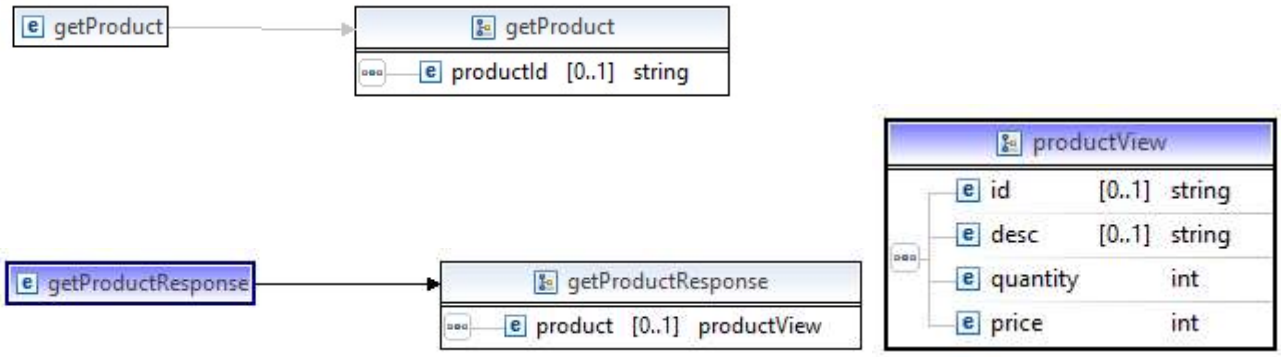
b) [0,6v] A secção *binding* do WSDL permite definir:

A. O tipo de dados XML das mensagens.
B. O endereço (URL) de invocação do serviço.
C. O protocolo a usar para transportar as mensagens.
D. A linguagem de programação a utilizar na implementação do serviço.

c) [0,6v] O endereço especificado no SupplierPort deste WSDL, cujo valor completo é `http://localhost:8081/supplier/endpoint`, terá que ser substituído quando o serviço for instalado em produção para ser usado por diversos clientes. Por que razão?

A. O protocolo HTTP não é suportado pelos Web Services.
B. O nome `localhost` referencia sempre a máquina local.
C. O porto 8081 não pode ser usado para comunicação com HTTP.
D. É obrigatório o uso de HTTPS nos Web Services.

d) O detalhe da operação `getProduct`, que complementa a informação anterior, é o seguinte:



A ferramenta wsimport permite gerar código Java para implementação do Web Service, a partir do WSDL. Apresente uma aproximação do código Java que é gerado pela ferramenta wsimport para:

i) [0,5v] Classe vista do produto (omita construtores, *getters* e *setters*)

```
public class ProductView {




}
```

ii) [0,5v] Assinatura do método correspondente à operação remota `getProduct`

Grupo IV – Tolerância a Faltas [4v]

Considere um sistema composto por clientes três serviços remotos: SA, SB e SC. Existem pelo menos dois clientes (C1, C2) que invocam operações destes serviços. Para maior tolerância a faltas, os serviços SA, SB e SC recorrem a diferentes soluções de replicação estudadas na disciplina:
- O SA usa Primary-Backup, com 2 réplicas (R1 – primário inicial, e R2).
- O SB usa Quorum Consensus, com 3 réplicas (R1, R2 e R3);
- O SC usa Gossip Architecture, com 3 réplicas (R1, R2 e R3).

1. No caso do protocolo Primary-Backup (serviço SA):
   a. [0,6v] De que forma é detetada da falta do R1?

   b. [0,8v] Qual é o tempo médio para a substituição do R1 após a deteção da falta? Apresente uma fórmula e descreva todos os seus componentes.

2. No caso do protocolo Quorum Consensus (serviço SB), considere que, num dado instante, o estado das réplicas é o seguinte:
   R1: <val=0; tag=<seq=1; cli=1>>
   R2: <val=100; tag=<seq=2; cli=1>>
   R3: <val=200; tag=<seq=3; cli=2>>

   a. [0,6v] Um cliente efetua uma leitura com o sistema no estado acima. Que valor(es) pode obter?

   b. [0,6v] Estando o sistema no estado acima, a mensagem <val=100; tag=<seq=2; cli=1>> é recebida por todas as réplicas. Qual o novo estado do sistema?

R1:
R2:
R3:

3. [0,7v] Comparando as opções de replicação usadas com o SA e SB, é evidente que a SA é mais barata pois exige menos máquinas para tolerar o mesmo número de falhas. Apresente uma razão plausível para o facto do SB recorrer a Quorum Consensus apesar do custo superior.

4. [0,7v] Comparando agora as opções de replicação usadas com o SB e SC, a solução usada no SC funciona mesmo em situações em que uma partição de rede isole temporariamente o cliente e uma réplica do resto do sistema, ao contrário da solução usada pelo SB.
   Apresente uma razão plausível para o facto do SB recorrer a Quorum Consensus apesar da desvantagem acima.

Grupo V – Transações Distribuídas [1 valor]

Considere um sistema de compras online em que cada utilizador pode juntar itens no seu carrinho de compras e, no final, fechar a compra conjunta desses itens junto dos respetivos fornecedores.

Cada fornecedor dispõe de um serviço remoto que permite efetuar a compra dos itens no seu inventário.

Para uma dada compra envolvendo 5 participantes (A,B,C,D,E), chega o momento da terminação atómica seguindo o protocolo é o 2-Phase Commit (2PC).

Indique qual a decisão tomada pelo coordenador em cada uma das seguintes situações.

1) [0,5v] Após enviar *canCommit*(tx), o coordenador recebeu voto *Yes* de todos os participantes exceto do E, cuja resposta não chegou ao coordenador ao fim do *timeout* definido pelo coordenador.

   A. Coordenador envia *doCancel* a todos.
   B. Coordenador envia *doCommit* a todos.
   C. Coordenador envia *doCommit* aos participantes que votaram *Yes* e *doCancel* a E.
   D. Coordenador não toma nenhuma decisão neste caso.

2) [0,5v] Após enviar *canCommit*(tx), o coordenador recebeu voto *Yes* de todos os participantes, incluindo E. Entretanto, E falhou temporariamente, antes de receber a decisão do coordenador.

   A. Todos os participantes cancelam a transação, incluindo E depois de recuperar.
   B. Todos os participantes confirmam a transação, incluindo E depois de recuperar.
   C. Os participantes A-D confirmam a transação e E cancela a transação assim que recuperar.
   D. Participantes não confirmam nem cancelam nesta situação, porque é necessário repetir a votação.

Grupo VI – Segurança [5 valores]

Considere novamente o sistema definido no grupo III – **Portal de compras e fornecedores**. Reveja a figura. Estão a ser usadas diferentes soluções de segurança para a comunicação entre os seguintes pares de entidades:

- Portal e Fornecedores <–> UDDI
- Clientes <–> Portal
- Portal <–> Fornecedores

1) A comunicação com o UDDI usa SOAP/HTTP e a autenticação do cliente é feita por nome e senha.
O servidor UDDI armazena o valor do resumo SHA-256 da senha secreta de cada utilizador. Esse resumo é designado por *passhash*.
Quando um cliente pretende consultar o UDDI, a mensagem leva o nome de utilizador e a *passhash* num cabeçalho da mensagem SOAP, tal como exemplificado de seguida:

```
<soap:envelope>
    <soap:header>
        <s:user>portal</s:user>
        <s:passhash>F13304121FEEABABCD131423FAB2FF10</s:passhash>
    </soap:header>
    <soap:body>
        <uddi:query>
            <uddi:queryString>Fornecedor%</uddi:queryString>
        </uddi:query>
    </soap:body>
</soap:envelope>
```

a) [0,6v] Um atacante consegue fazer um ataque de intermediário (*man-in-the-middle*) trocando a *query* enviada pelo cliente por outra? Justifique.

b) [0,7v] Que modificações deverá fazer à mensagem para garantir **confidencialidade** da *query* a enviar para o UDDI de modo a que este possa depois responder?

A. Remover: *passhash* e *query*. Acrescentar: *query* cifrada com chave derivada da *passhash*.
B. Remover: *passhash* e *query*. Acrescentar: MAC da *query* calculado com chave derivada da *passhash*.
C. Remover: *query*. Acrescentar: nova chave AES-128 gerada no momento pelo cliente de forma aleatória, *query* cifrada com a nova chave.
D. Remover: *query string*. Acrescentar: resumo SHA-256 da *query string*.

2) A comunicação dos clientes com o portal de compras está a ser feita através de HTTPS, tendo o Portal de Compras um certificado digital de chave pública em utilização com o seguinte conteúdo:

Issued To
Common Name (CN): Portal de Compras
Organization (O): Portal de Compras, Lda.
Serial Number: 12521043030
Public Key Algorithm: RSA-2048
Public Key: b7 36 55 e5 a5 5d 18 30 e0 da 89 54 91 fc c8 c7 … (2048 bits + 3 bits exponent)
Issued By
Common Name (CN): Brand New CA
Organization (O): Brand New Certificates Company
Period of Validity
Begins on: 2019-08-01, *Expires on:* 2020-07-31
Fingerprints:
SHA-1 Fingerprint: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1
SHA-256 Fingerprint: **not available**
Signature:
Algorithm: SHA-1 with RSA encryption
Value: 0c 41 97 c2 1a 86 c0 22 7c 9f fb 90 f3 1a d1 03 … (256 bytes)

Nota importante: à data de hoje, a *Brand New CA* apenas é reconhecida pelo navegador Apple Safari.

a) [0,7v] Quem produziu o *Signature Value* (valor da assinatura)?
Que funções criptográficas e que chaves foram necessárias para o fazer?

b) O certificado acima tem três problemas. Identifique dois dos problemas e explique-os sucintamente para justificar a sua resposta.
i) [0,6v] Primeiro problema

ii) [0,6v] Segundo problema

3) A comunicação do portal com os fornecedores usa SOAP/HTTP mas a autenticação usa **Kerberos v5**.

a) [0,6v] Que servidores são necessários para permitir a utilização de Kerberos na versão indicada? Indique, sucintamente, qual a função de cada um deles.

b) [0,6v] Descreva o conteúdo e a proteção criptográfica do **autenticador** enviado do portal para o Fornecedor 2 quando envia um pedido. Identifique todas as funções criptográficas e chaves utilizadas na sua construção.

c) [0,6v] *"O uso de Kerberos implica a sincronização de relógios entre todos os servidores envolvidos."* Concorda com a afirmação? Justifique.
