Número: Nome:

Sistemas Distribuídos

Faculdade de Ciências e Tecnologia
2019/20
Exame - Época Normal
Versão A
sem consulta ; duração total: 2h30

As respostas erradas às perguntas V/F descontam até o equivalente ao valor da resposta certa correspondente. Para as perguntas de escolha de múltipla, o desconto é de $1/(n-1)$, com n o número de opções. A penalização acumula apenas no contexto da mesma pergunta. Em cada pergunta, a primeira resposta errada não desconta.

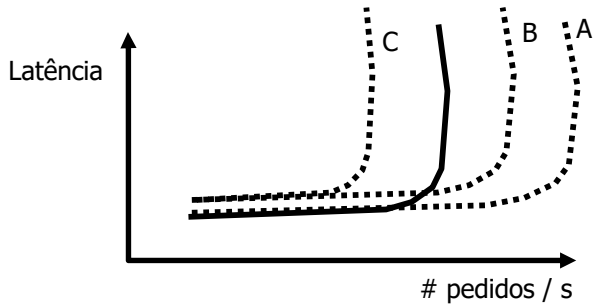
Questão 1
Para cada uma das seguintes afirmações, indique se é `[V]`erdadeira ou `[F]`alsa ou escolha a resposta apropriada, no caso das perguntas de escolha múltipla.

1. ____ Se ao fim de três tentativas de contacto, um servidor não responder, sabe-se que o servidor falhou. (V/F)
2. ____ Se um cliente não receber resposta ao seu pedido, sabe que o servidor não executou o pedido. (V/F)
3. ____ Para qualquer aplicação de código aberto (open-source), é sempre possível usar parte do seu código num aplicação que estejamos a desenvolver. (V/F)
4. ____ Um sistema aberto é um sistema cujo especificação e algoritmos são conhecidos. (V/F)
5. ____ Considere que tem um sistema tolerante a falhas (e.g.do tipo fail-stop), que tolera f falhas. Quando o número de falhas é superior a f, o que é que desejável e razoável assumir do sistema: (A) todas as operações param de executar; (B) algumas operações não podem executar, enquanto outras podem; (C) todas as operações continuam a executar; (D) nenhuma das anteriores. NOTA: Considere um sistema semelhante ao desenvolvido no projeto. (A/B/C/D)
6. ____ Para detetar uma falha bizantina (ou arbitrária) dum servidor, será tipicamente necessário que um cliente comunique com múltiplos servidores. (V/F)
7. ____ O UDP é um mecanismo de comunicação volátil. (V/F)
8. ____ O TCP é um mecanismo de comunicação síncrono. (V/F)
9. ____ Para receber notificações num cliente Web, a técnica de comunicação mais apropriada de entre as seguintes seria: (A) pedidos HTTP normais; (B) pedidos HTTP assíncronos; (C) Web Sockets. (A/B/C)

Questão 2
Para cada uma das seguintes afirmações, indique se é `[V]`erdadeira ou `[F]`alsa ou escolha a resposta apropriada, no caso das perguntas de escolha múltipla.

10. ____ Se pretendesse implementar um sistema de nomes usando um sistema peer-to-peer, seria mais eficiente fazê-lo usando: (A) um sistema peer-to-peer estruturado; (B) um sistema peer-to-peer não estruturado; (C) não faria diferença significativa a opção. (A/B/C)
11. ____ Qual das seguintes diria que é a diferença mais importante entre um sistema peer-to-peer (P2P) estruturado e não estruturado: (A) num sistema P2P estruturado é mais eficiente encaminhar uma mensagem para um nó, dado o seu identificador; (B) num sistema P2P estruturado é mais eficiente encaminhar uma mensagem para todos os nós do sistema; (C) os algoritmos dum sistema P2P estruturado são tipicamente mais simples de implementar. (A/B/C)
12. ____ No sistema BitTorrent, o facto dos peers obterem blocos aleatoriamente (i.e., sem ser por ordem) contribui principalmente para que: (A) um novo peer consiga começar a receber o ficheiro; (B) que os peers participem de forma equilibrada na partilha do ficheiro; (C) que um peer consiga manter a velocidade de transferência até ao fim da transferência dum ficheiro; (D) as três anteriores. (A/B/C/D)
13. ____ Hoje em dia, é comum as aplicações web executarem parte da funcionalidade no cliente (usando JavaScript). Esta aproximação pode permitir a uma aplicação, até certo ponto, mascarar falhas de comunicação. (V/F)
14. ____ Os servidores na periferia, como os servidor de CDN, podem ajudar a defender um sistema de ataques distribuídos de negação de serviço (DDoS) ? (V/F)
15. ____ Numa aplicação distribuída desenhada com base numa arquitetura em três camadas, a parte mais difícil de tornar tolerante a falhas é: (A) a camada da lógica da aplicação; (B) a camada dos dados; (C) as duas anteriores. (A/B/C)
16. ____ O objetivo dos testes unitários é testar a funcionalidade duma componente de forma isolada. (V/F)

17. Avaliaram-se várias versões dum sistema que tem operações de leitura e operações de escrita (50% de escritas e 50% de leituras). As versões avaliadas incluiam uma versão base, com apenas um servidor (linha contínua), uma versão com o servidor particionado e uma versão com o servidor replicado (ambas com o mesmo número total de servidores). No gráfico seguinte, o eixo vertical representa a latência média das operações e o eixo horizontal representa o número total de operações executadas no sistemas. Nesse conte¡xto, indique:
Qual a linha que representa o servidor replicado? ____ (A/B/C)
Qual a linha que representa o servidor particionado? ____ (A/B/C)
Sugestão: considere o custo de executar as diferentes operações num sistema replicado e num sistema particionado.



Questão 3
Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa ou escolha a resposta apropriada, no caso das perguntas de escolha múltipla.

18. ____ No sistema Java RMI, quando um método tem um parâmetro do tipo X, o cliente pode passar como valor desse parâmetro um objeto do tipo Y, tal que Y estende X. (V/F)

19. ____ O XML Schema permite definir os elementos que podem aparecer num documento XML. (V/F)

20. ____ A escolha do mecanismo de serialização tem pouco impacto no desempenho duma aplicação distribuída. (V/F)

21. ____ No suporte REST disponível no Java e usado nos trabalho práticos, se se registar no servidor o nome da classe, como no exemplo seguinte, durante a vida do servidor serão criadas múltiplas instâncias do recurso para atender diferentes pedidos. (V/F)

```
@Path("/myserver")
public class MyResource {
    ...
}

...
ResourceConfig config = new ResourceConfig();
config.register(MyResource.class);
```

22. ____ Definir todos os métodos dos recursos REST como synchronized permite, em todas as circunstâncias, garantir o correto controlo da concorrência entre pedidos concorrentes. (V/F)

23. ____ As interações REST devem ser *stateless*, algo que, potencialmente, permite às aplicações obter melhor desempenho da infra-estrutura de *caching* HTTP.

24. ____ O WSDL exposto por um programa desenvolvido em Java, pode ser usado para criar um cliente noutra linguagem (e.g. C). (V/F)

25. ____ A semântica de invocação dos WebServices SOAP, por omissão, é "no máximo uma vez" (at most once). (V/F)

26. ____ No âmbito dos WebServices SOAP, o UDDI pode funcionar como um serviço de nomes. (V/F)

Número: Nome:

Questão 4
Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa ou escolha a resposta apropriada, no caso das perguntas de escolha múltipla.

27. ____ Dados dois relógios vetoriais, v_1 e v_2, é possível saber saber se os eventos relativos a v_1 e v_2 são concorrentes. (V/F)
28. ____ No protocolo de replicação primário/secundário, quando se replica uma operação, se o primário ficasse à espera da confirmação de todos os secundários, não seria capaz de tolerar falhas. (V/F)
29. ____ No sistema Coda, é possível que dois servidores que viram as mesmas escritas tenham diferentes vetores-versão. (V/F)
30. ____ No sistema de caching usado no NFS, o servidor tem de manter informação sobre os clientes que têm ficheiros em cache. (V/F)
31. ____ No sistema de caching que usa *opportunitic locks*, o servidor tem de manter informação sobre os clientes que têm ficheiros em cache. (V/F)
32. ____ O sistema Zookeeper replica os dados usando um modelo de consistência eventual. (V/F)
33. ____ No algoritmo de eleição de primário estudado, com recurso ao sistema Zookeeper, se se selecionasse como primário o servidor cujo nome fosse o maior (na ordem lexicográfica), seria possível ter uma configuração em que (temporariamente) houvesse vários nós que pensem que são o primário. (V/F)
34. ____ A replicação primário/secundário, quando não há mudanças na filiação (membership), pode ser implementada por recurso a um sistema de comunicação em grupo desde que este ofereça uma semântica de ordenação (escolha a primeira resposta verdadeira): (A) sem ordem; (B) FIFO; (C) causal; (D) total. (A/B/C/D)
35. ____ Num sistema que utilize geo-replicação, a utilização dum modelo de consistência fraca permite uma melhor latência do que quando se usa um modelo de consistência forte. (V/F)

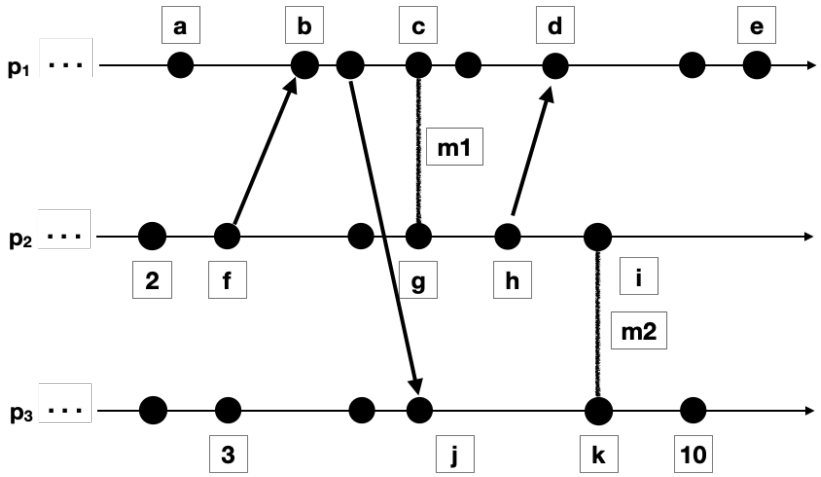
Questão 5
Para cada uma das seguintes afirmações, indique se é [V]erdadeira ou [F]alsa ou escolha a resposta apropriada, no caso das perguntas de escolha múltipla.

36. ____ Para um sistema ser *dependable* (confiável) não basta ser seguro. (V/F)
37. ____ Em segurança, a autenticação é um mecanismo que só tem utilidade para efeitos de controlo de acessos. (V/F)
38. ____ Num sistema distribuído, se a implementação da *trusted computing base* estiver incorreta, então o sistema distribuído não será seguro. (V/F)
39. ____ OAuth é uma forma segura de um utilizador se autenticar perante um serviço A, utilizando a sua autenticação num serviço B, sem que A conheça as credenciais desse utilizador em B. (V/F)
40. ____ As funções de síntese seguras têm melhor desempenho do que os algoritmos de cifra com chave simétrica. (V/F)
41. ____ Quando se usa o algoritmo de cifra por blocos encadeados, o criptograma (ciphertext) pode revelar os padrões da mensagem em claro (plaintext). (V/F)
42. ____ O algoritmo de Diffie-Hellman dá suporte à noção de *segurança futura perfeita*. (V/F)
43. ____ No protocolo TLS, o servidor envia para o cliente um certificado X.509 que contém a sua chave pública. (V/F)
44. ____ Num computador, a lista de certificado das entidades de certificação faz parte da *trusted computing base*. (V/F)

Número: Nome:

Questão 6

Considere o seguinte diagrama temporal, onde está representado um padrão de comunicação ponto-a-ponto, envolvendo os processos p1, p2 e p3. Para as mensagens, m1 e m2, desconhece-se o sentido da comunicação. Os eventos nos processos estão assinalados por círculos negros. Cada evento tem associado uma caixa, cujo valor é uma estampilha de um relógio de Lamport, de valores inteiros, atualizado pelo menor incremento possível.



Responda a cada pergunta de forma independente, escolhendo a resposta que pode ser explicada com base nos valores presentes no diagrama e as condições enunciadas na pergunta. Responda a todas as questões.

45. ____ O valor de f é: (A) 3; (B) 6; (C) 7; (D) nenhum dos anteriores. (A/B/C/D)
46. ____ O menor valor possível para i é: (A) 6; (B) 7; (C) 8; (D) nenhum dos anteriores. (A/B/C/D)
47. ____ O menor valor possível para a é: (A) 1; (B) 2; (C) 5; (D) nenhum dos anteriores. (A/B/C/D)
48. ____ O maior valor possível para e é: (A) 10; (B) 12; (C) 13; (D) nenhum dos anteriores. (A/B/C/D)
49. ____ Independentemente do sentido de m1 e m2, o evento 3 *aconteceu antes* do evento e. (V/F)
50. ____ Independentemente do sentido de m1 e m2, o evento a *aconteceu antes* do evento i. (V/F)
51. ____ Independentemente do sentido de m1 e m2, o evento 2 *aconteceu antes* do evento 10. (V/F)
52. ____ Se a direção de $m2$ for $i \rightarrow k$, a direção de $m1$ terá de ser $g \rightarrow c$. (V/F)

Questão 7

É comum colocar-se um proxy próximo dum servidor, para fazer caching das respostas do servidor. Quais as motivações para o fazer? Compare esta solução com a solução alternativa de criar réplicas do servidor, apresentando vantagens e desvantagens de cada uma.

Questão 8

Considere que pretende implementar um jogo online de realidade aumentado, do tipo *Pokemon Go*. Neste tipo de jogo há locais (e.g. salas de treino) e objetos que estão associados a uma localização no mundo real. Um jogador pode interagir com um local (resp. objeto) se estiver na localização física desse local (resp. objeto) no mundo real. Por exemplo, um utilizador pode apanhar um objeto ou treinar numa sala de treino.

Pretende-se que um jogo tenha o maior número de jogadores possível, estando estes espalhados pelo mundo. Vamos supor um mundo pré-COVID-19, em que as pessoas podiam viajar entre diferentes continentes.

Para suportar esta plataforma, irá ser necessário ter um serviço que mantém o estado dum jogo. Este serviço registará os jogadores que estão a jogar, a sua posição, a posição e estados dos locais e objetos, e a interação dos jogadores com os locais e objetos. Algumas das operações fornecidas pelo serviço serão as seguintes:

(1) adicionar um jogador;
(2) remover um jogador;
(3) criar um objeto / local numa dada posição;
(4) registar a posição dum utilizador – esta operação devolve os locais e objeto na vizinhança;
(5) registar uma interação com um local / objeto – esta operação devolve um booleano a indicar se a interação foi bem sucedida (e.g. quando se tenta apanhar um objeto, pode devolver *false* se outro utilizador o apanhou antes);
(6) obter informação sobre os jogadores/locais/objetos na vizinhança duma dada localização.

a) Considere que irá recorrer à *cloud* para implementar as funcionalidades da plataforma, tendo ao seu dispor um conjunto de cinco centros de dados – Europa, África, América do Norte, América do Sul e Ásia. Discuta se faz sentido particionar e/ou replicar a informação do serviço que mantém o estado do jogo? Justifique, discutindo em caso afirmativo como particionaria e/ou replicaria essa informação. (Evite afirmações genéricas, responda para o caso concreto desta pergunta.)

b) Faria sentido usar um sistema CDN para completar a solução proposta na resposta anterior, assumindo um sistema de CDN em que cada provedor de Internet (e.g. em Portugal, seriam Meo, Vodafone, Nos, etc.) teria um ponto de presença da CDN? Justifique, discutindo que operações poderiam ser suportadas nesses sistemas e quais não poderiam ser. (Evite afirmações genéricas, responda para o caso concreto desta pergunta.)

Número: Nome:

Questão 9

Considere a seguinte alteração ao protocolo primário/secundário para processar uma operação de escrita: (1) cliente envia operação de escrita para o primário; (2) primário executa a operação e envia resultado ao cliente; (3) primário envia operação para os secundários; (4) ao receber uma operação do primário, caso detete que não recebeu alguma operação anterior, secundário envia pedido da operação em falta ao primário; caso contrário, executa a operação e envia resultado diretamente ao cliente; (5) cliente considera a operação concluída com sucesso quando recebe $n/2 + 1$ respostas, com n o número de secundários (assumindo que se toleram $f = n/2$ falhas). Assumindo que só há operações de escrita, discuta se esta modificação permite manter a correção do protocolo. Em caso afirmativo, discuta as vantagens/desvantagens face à solução original; em caso negativo, indique em que situação não se mantém a correção do sistema.

Questão 10
Considere o contexto de um sistema de difusão de conteúdos multimédia. Neste sistema, um servidor `S` difunde para um cliente `C` um conteúdo `M` (de grandes dimensões). Para ajudar a garantir a segurança do sistema, existe um servidor de segurança (`SS`) que partilha com o servidor e com cada cliente uma chave simétrica (Kss para o servidor `S`, Ksc para o cliente).

Pretende-se criar um protocolo que permita difundir um ficheiro de `S` para `C` de forma segura, i.e., garantindo o secretismo das mensagens e do conteúdo do ficheiro e a autenticação dos parceiros de comunicação (i.e., `C` deve ter a certeza que recebeu o ficheiro de `S` e `S` deve ter a certeza que apenas `C` pode obter o conteúdo do ficheiro). A solução deve minimizar a informação transmitida na rede e o poder computacional necessário para executar o protocolo. O protocolo deve ter, no máximo, 3 mensagens, efetuando a seguinte interação: $S \rightarrow SS$; $SS \rightarrow C$; $S \rightarrow C$.

1. S → SS :
2. SS → C :
3. S → C :

Indique a melhor resposta, tendo em conta o objetivo do protocolo e os pressupostos enunciados.
Responda a todas as questões.

53. ____ O passo 1 deve ser preenchido com:
(A) $\{S, N, M\}_{Kss}$
(B) $S, \{N, M\}_{Kss}$
(C) $\{S, H(M+N), K\}_{Kss}$
(D) $S, \{H(M+N)\}_{Kss}$
(E) $S, \{H(M+N), K\}_{Kss}$
(F) nenhuma das anteriores

54. ____ O passo 2 deve ser preenchido com:
(A) $\{S, N, M\}_{Ksc}$
(B) $S, \{N, M\}_{Ksc}$
(C) $\{S, H(M+N), K\}_{Ksc}$
(D) $S, \{H(M+N), K_{ss}\}_{Ksc}$
(E) $S, \{H(M+N), K\}_{Ksc}$
(F) nenhuma das anteriores

55. ____ O passo 3 deve ser preenchido com:
(A) $H(M+N)$
(B) $\{H(M+N)\}_{Kss}$
(C) $\{H(M+N)\}_{K}$
(D) $\{N, M\}_{Kss}$
(E) $\{N, M\}_{K}$
(F) nenhuma das anteriores

56. Caso se pretendesse que o servidor `S` tomasse conhecimento que o cliente `C` tinha obtido a mensagem, indique que mensagem é que o cliente deveria enviar ao servidor. Justifique.

Questão 11
O João mora em Lagoas e está farto de estar em casa por causa do COVID. Por isso decidiu que tinha de aproveitar a vida ao máximo indo a festas na sua zona de residência. O João decidiu montar um sistema, que interage com o uma API Rest de uma rede social chamada LivroDasCaras para obter informação sobre festas a que os seus amigos vão. Para tal ele fez uma aplicação que interage com o LivroDasCaras e que obtém uma lista de todos os (novos) eventos públicos em que pelo menos um dos seus amigos se registou.

Mas o João não quer perder tempo, e prefere ir a festas com o máximo número de pessoas possível, no mínimo 100, porque quer rever toda a gente o mais depressa possivel. Por isso, sempre que a sua aplicação identifica um novo evento, ele invoca a função (ver código seguinte) em que passa o identificador único do evento. Essa função vai obter os detalhes do evento para verificar se pelo menos 100 pessoas já disseram que vão a festa, e no caso desse limite ser alcançado, invoca uma função que lhe envia um SMS (função partyTime).

Deve notar que: i) a rede social LivroDasCaras ainda é recente, sendo que a sua interface REST opera sobre http e não requer autenticação do cliente; e ii) o João quer que o seu programa execute sem parar no seu computador, mesmo enquanto ele anda a passear pela rua, ou está noutra festa, e não quer perder festas.

57. Descreva pelas suas palavras o que é que o código da função checkAwesomeParty apresentado de seguida faz (A figura apresenta a especificação de uma classe auxiliar).

58. Como já deve suspeitar, o João não frequentou a disciplina de SD, e por isso o seu código apresenta algumas fragilidades. Identifique 2 aspetos no código do João que podiam ser melhorados e descreva como é que cada um dos aspetos identificados podem fragilizar a aplicação do João (PS: O João experimentou o código na máquina dele uma vez e funcionou).

59. A rede social LivroDasCaras parece ter mecanismos de segurança adequados? Quais são os problemas potenciais que têm, as suas implicações, e como poderiam ser endereçados?

```
21  private class EventDetails {
22      public long eventID;
23      public String title;
24      public String date;
25      public String time;
26      public int attendees;
27      public String location;
28
29      public EventDetails() { }
30  }
31
32  public void checkAwesomeParty(String eventID) throws IOException {
33
34      ClientConfig config = new ClientConfig();
35      Client client = ClientBuilder.newClient(config);
36
37      WebTarget target = client.target( "http://livrodascaras.pt/" )
38              .path( "eventos" ).path(eventID);
39
40      Response r = target.request()
41              .accept(MediaType.APPLICATION_JSON)
42              .get();
43
44      EventDetails details = r.readEntity(EventDetails.class);
45
46      if(details.attendees >= 100) {
47          //the following methods sends an SMS with the details of event
48          partyTime(details.eventID, details.title, details.location, details.date, details.time);
49      }
50  }
```

Número: Nome:

RASCUNHO