Número: Nome:

Sistemas Distribuídos

Faculdade de Ciências e Tecnologia
2017/18
Exame de Recurso - PARTE 2
sem consulta - Duração total: 60 + 120 minutos

Questão 1

Para cada uma das seguintes afirmações indique na folha de respostas se é [V]erdadeira ou [F]alsa. Em caso de dúvida, justifique a resposta no verso da folha de respostas. As respostas erradas descontam.

1. Um conjunto de componentes de software e hardware que se coordenam entre si exclusivamente através da troca de mensagens, mesmo que e o transporte das mesmas envolva a partilha de memória, podem ser considerados um sistema distribuído.
2. Uma arquitectura baseada na noção de servidor particionado distribui as várias funcionalidades do sistema distribuído por várias máquinas a fim de distribuir a carga.
3. Um bom motivo para um sistema distribuído adoptar uma arquitectura baseada na noção de servidor geo-replicado poderá ser aumentar o desempenho das escritas;
4. As primitivas de comunicação *anycast* não podem suportar uma semântica de entrega do tipo FIFO;
5. Segundo a definição, uma primitiva de comunicação em grupo só pode ser considerada fiável se uma mensagem que foi enviada for entregue em todos os processos;
6. Um *proxy* alojado junto ao cliente permite mascarar falhas de conectividade e que este trabalhe em modo desligado/*offline*;
7. Um *proxy* alojado junto ao servidor permite que clientes obsoletos possam ser servidos por versões mais recentes do servidor;
8. Um sistema P2P, cuja topologia forma um trie com base no padrão binário dos identificadores dos nós, deve ser classificado como estruturado;
9. Num sistema P2P como o Chord, é possível implementar uma primitiva de comunicação broadcast que entregue cada mensagem uma e uma só vez em cada nó;
10. Não é possível implementar uma primitiva de comunicação em grupo com uma semântica de entrega compatível com a ordem total sem que todas as mensagens sejam primeiro enviadas a um nó central para que este as ordene;

Questão 2

Para cada uma das seguintes afirmações indique na folha de respostas se é [V]erdadeira ou [F]alsa. Em caso de dúvida, justifique a resposta no verso da folha de respostas. As respostas erradas descontam.

11. Em REST é possível implementar uma semântica de invocação "pelo menos uma vez"(*at least once*).
12. A invocação remota em .NET Remoting não necessita de usar o conceito de IDL.
13. Em REST, a passagem de dados envolve sempre a codificação dos mesmos no formato JSON.
14. ProtoBuf é um sistema de codificação de dados que usa um formato binário.
15. A serialização de objetos em Java suporta classes de objetos recursivas, ie., com referências para objetos dessa mesma classe.
16. Nos web services SOAP, o WSDL obtido de um dado servidor só pode ser usado para invocar o mesmo servidor.

Questão 3

Leia com atenção as seguintes afirmações e assinale na folha de respostas se são verdadeiras ou falsas. Respostas incorretas descontam. Em caso de dúvida, justifique.

17. Para um sistema ser confiável (*dependable*) precisa de ser tolerante a falhas;
18. O sistema distribuído com a *trusted computing base* "menor"tenderá a ser o mais seguro;
19. O mecanismo OAuth fornece uma forma de controlo de acessos;
20. Um canal seguro é um canal que está imune aos ataques de negação de serviço (distribuídos).
21. Para comprimir o tráfego de um canal seguro, é indiferente a ordem pelas quais as operações de compressão e de cifra são realizadas;
22. Sozinha, a criptografia assimétrica só é adequada para cifrar o conteúdo de ficheiros de dados pequenos;

23. Cifrar com uma chave assimétrica privada uma mensagem, garante a confidencialidade da mesma;
24. Um certificado de revogação de chaves públicas de uma CA (autoridade de certificação) deve ser mantido em segredo;
25. O resultado de aplicar uma função de síntese a uma mensagem é proporcional à dimensão da mensagem;
26. O algoritmo de Diffie-Hellman permite implementar algo a que se denomina segurança futura perfeita;
27. Entre dois eventos, é possível que o evento com a maior estampilha tenha ocorrido em tempo físico antes do outro (com a estampilha menor).
28. Em geral, a replicação primário/secundário é uma forma eficaz de equilibrar a carga de um sistema distribuído onde as escritas dominam;
29. Um sistema distribuído não pode tolerar falhas se não implementar replicação;
30. O desempenho de uma solução de caching tende a aumentar se as garantias de consistência dos dados forem relaxadas;
31. Uma solução de replicação baseada na consistência eventual permite que nem todas as réplicas passem pelos menos estados;
32. Para as escritas, o sistema de ficheiros NFS faz a gestão da sua cache com base em *opportunistic locks*;
33. No sistema de ficheiros CIFS, quando existem dois clientes com intenção de escrever o ficheiro ao mesmo tempo, este deixa de pode ser colocado em cache;
34. No sistema de ficheiros Coda, em alguns casos a resolução de conflitos é automática;
35. Um serviço de nomes pode substituir um serviço de directório, o contrário não é verdade;
36. Um nome puro é um nome que não contém informação de localização, logo um URN não pode ser um nome puro.
37. Um nome puro é um nome que não contém informação de localização, aplicar uma função de síntese a um nome, permite tornar qualquer nome num nome puro.

Número: Nome:

Questão 4

Considere o Youtube que permite o carregamento de vídeos, produzidos pelos próprios utilizadores, e sua, posterior visualização por uma audiência global. Neste sistema, vídeos de autores populares podem acumular milhões de visualizações em pouco tempo, enquanto uma enorme massa de vídeos, não passa de umas poucas centenas ao final de vários anos. A visualização dos vídeos gera ingressos ao dono da plataforma através da publicidade que é embebida nos vídeos durante a sua reprodução. Estes lucros são partilhados com os autores que, para tal, são incentivados a produzir conteúdo original, com regularidade, sob pena de caírem no esquecimento e verem o seu rendimento desaparecer. É frequente os utilizadores "profissionais"da plataforma apelarem à audiência para que subscreva o seu canal, deixe comentários, e melhor ainda, peça para ser notificada quando existe novo conteúdo. Para além de conseguir criar um vídeo que se torna viral, esta é a forma sustentada de um canal conseguir criar uma audiência regular e começar a aparecer nas listas de vídeos recomendados que a plataforma apresenta aos utilizadores. Hoje em dia, os conteúdos do Youtube podem ser consumidos numa grande variedade de equipamentos, desde computadores pessoais, dispositivos móveis e televisões inteligentes, espalhados por todo o planeta.

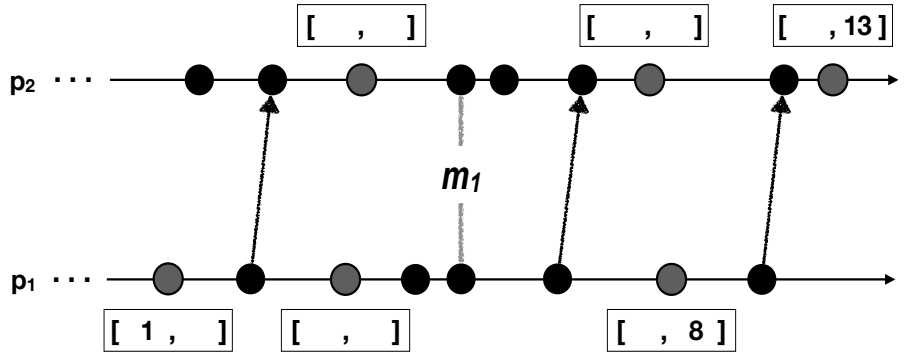
Para cada questão isoladamente, assinale QUAL das opções produz a afirmação mais correta e/ou o argumento mais forte, supondo que serão as máquinas que recebem os pedidos dos clientes que alojam os vídeos e os outros dados da plataforma. Respostas claramente erradas descontam.

38. Youtube utilizará um arquitectura baseada na noção de servidor particionado, principalmente para:
    A) distribuir a carga de (streaming) de um vídeo que se torna viral;
    B) endereçar problemas de escalabilidade da plataforma;
    C) distribuir as várias funcionalidades disponíveis por várias máquinas;
    D) distribuir os comentários de um vídeo que se torna viral;
    E) permitir o upload e o download de vídeos em simultâneo;
39. A noção de servidor replicado no Youtube:
    A) permitará garantir que qualquer vídeo está sempre disponível;
    B) permitará distribuir a carga de (streaming) de um vídeo que se torna viral;
    C) não deverá ser usada para vídeos pouco populares;
    D) será útil para todos os vídeos e dados da plataforma;
    E) será adequada apenas para os vídeos que se tornam virais;
40. A noção de servidor geo-replicado no Youtube:
    A) permite melhorar a qualidade do serviço no seu todo porque reduz a latência;
    B) devido ao buffering, tem pouco impacto no streaming ou upload dos vídeos;
    C) aplica-se a todos os vídeos por igual;
    D) é especialmente eficaz para os videos muito comentados;
    E) é essencial para permitir oferecer publicidade personalizada aos utilizadores de cada país;
41. Para o Youtube, explorar a noção de caching:
    A) beneficia da natureza imutável dos vídeos;
    B) não pode ser aplicada aos anúncios porque estão sempre a mudar;
    C) não pode basear-se em estampilhas físicas;
    D) é uma forma eficaz para lidar com vídeos que se tornam virais;
    E) só é útil para os vídeos que um dado utilizador vê muitas vezes repetidas;

Número: Nome:

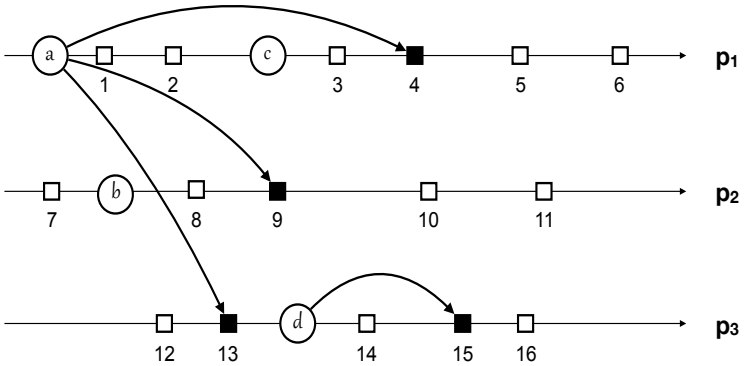
Questão 5

Considere o seguinte diagrama temporal correspondente a um sistema composto por dois processos: p_1 e p_2. As setas indicam eventos de comunicação ponto-a-ponto, uni-direcionais entre as componentes do sistema. m_1 é uma mensagem para a qual a direcção de envio e recepção foi suprimida. Os valores contidos, nas caixas junto aos eventos, correspondem a estampilhas de um relógio de vectorial. Considerando que o incremento mínimo é de 1 unidade, preencha os valores em falta das estampilhas, utilizando para cada entrada o valor máximo admissível. (Assuma o que achar necessário relativamente ao passado do sistema que não está representado no diagrama.)



Questão 6

Considere o seguinte diagrama que ilustra um padrão de comunicação em grupo, envolvendo 3 processos: p_1, p_2 e p_3. No total, são enviadas 4 mensagens: $\{a, b, c, d\}$, usando a mesma primitiva de comunicação. As setas indicam o momento em que ocorre a entrega de uma mensagem num dado processo. Para a mensagem a, esse momento está fixado nos 3 processos; para a mensagem d, apenas para o processo p_3. Para as demais situações, o momento de entrega está em aberto (e poderá ser identificado por um número). A comunicação é fiável e todos os processos deverão receber cada uma das mensagens.



Para cada questão isoladamente, assinale quais das opções são ou produzem afirmações verdadeiras. Respostas erradas descontam.

42. Para respeitar a ordem FIFO, a entrega da mensagem b em p_1:

A) só pode ocorrer em 4 ou 5 B) pode ocorrer em 1, 2, 3, 5 ou 6 C) deve ser entregue antes de c, mas depois de a
D) deve ser entregue entre a e c E) se c for entregue em 3, deve ser entregue em 1 ou 2

43. Para não violar a ordem CAUSAL, a entrega da mensagem d:

A) não pode ocorrer em 1 ou 2 B) pode ocorrer em 1, 2, 3, 5 ou 6 C) deve ser entregue antes de c, mas depois de a
D) deve ser entregue entre a e c E) se c for entregue em 3, d deve ser entregue em 1 ou 2

44. Supondo que c é entregue em 12, então uma semântica de entrega que satisfaz a ordem TOTAL :

A) obriga que b não possa ser entregue em 8 B) então se b for entregue em 14, obriga que d seja entregue em 6
C) determina que d não pode ser entregue em 10 D) determina que b não pode ser entregue em 16
E) não pode ser respeitada

45. Uma semântica de entrega compatível com uma ordem TOTAL CAUSAL:

A) não pode ser satisfeita pelo diagrama apresentado B) obriga que b seja a primeira mensagem entregue
C) c pode ser entregue antes de d D) c não pode ser entregue em 14
E) d poder ser entregue antes de c

Número: Nome:

Questão 7

A Alice pretende enviar uma mensagem secreta à Carol que se encontra em parte incerta. Como não tem contato direto com a Carol, a Alice precisa da ajuda de terceiros. O Bob e a Mallory prometeram ajudar, mas a Alice desconfia que um dos dois não é de confiança, só não sabe é quem. Infelizmente, a Alice não tem nenhum segredo partilhado previamente com a Carol, nem conhece a sua chave pública. Por isso, pensou em dividir a mensagem em duas partes, M_1 e M_2 que a Carol terá que juntar para poder reconstruir a mensagem original M. Se tudo correr bem, receberá da Carol uma prova de que esta leu a mensagem.

1. Alice → Bob: $\{N_a, M_1\}_{K_2}$, $\{\ \boxed{}\ \}_{K_{pubB}}$;
2. Alice → Mallory: $\boxed{}$, $\{\ \boxed{}\ \}_{K_{pubM}}$, $\boxed{}$;
3. Bob → Carol: $\boxed{}$, $\{K_1\}_{K_{pubC}}$;
4. Mallory → Carol: $\{N_b, M_2\}_{K_1}$, $\boxed{}$;
5. Carol → Alice: $\boxed{}$;

Ajude a Alice a entender e a completar o seguinte protocolo, de modo a fazer chegar a mensagem secreta à Carol de forma segura, escolhendo para cada uma das seguintes perguntas a melhor opção (ou melhores opções). Respostas erradas descontam.

46. No passo 1, a caixa deve ser preenchida com:

A) M_2 B) K_s C) $H(M_1)$ D) K_1 E) K_2

47. No passo 2, a primeira caixa deve ser preenchida com:

A) $\{N_a, M_2\}_{K_1}$ B) $\{N_b, M_2\}_{K_1}$ C) $\{N_a, M_1\}_{K_2}$ D) $\{N_b, M_1\}_{K_2}$ E) $\{N_b, M_2\}_{K_{pubC}}$

48. No passo 2, a segunda e a terceira caixa devem ser preenchidas, respetivamente, com:

A) M_2 e $H(M_1 + M_2)$ B) $H(M_1)$ e K_{pubA} C) K_s e N_a D) K_1 e N_b E) K_2 e nada

49. No passo 3, a caixa deve ser preenchida com:

A) $\{N_a, M_2\}_{K_1}$ B) $\{N_b, M_2\}_{K_1}$ C) $\{N_a, M_1\}_{K_2}$ D) $\{N_b, M_1\}_{K_2}$ E) $\{N_b, M_2\}_{K_{pubC}}$

50. No passo 4, a caixa deve ser preenchida com:

A) $\{K_1\}_{K_{pubC}}$ B) $\{K_1\}_{K_{pubM}}$ C) $\{K_2\}_{K_{pubC}}$ D) $\{K_2\}_{K_{pubM}}$ E) K_2

51. No passo 5, a caixa deve ser preenchida com:

A) $\{H(M + N_a + N_b)\}_{K_{privC}}$ B) $H(M_1 + N_b - 1)$ C) $H(M_2 + N_a - 1)$ D) $\{H(M)\}_{K_{privC}}$ E) $H(M + Na + Nb)$

52. No protocolo, N_a e N_b podiam ser omitidos se:

A) a Carol não precisasse de confirmar M B) só enviar M uma vez à Carol C) confiar no Bob
D) confiar na Carol E) não desconfiar da Mallory

53. O protocolo garantirá que só a Carol lerá a mensagem da Alice, apenas se:

A) a Mallory não interceptar a mensagem enviada no passo 1 B) o Bob não interceptar a mensagem enviada no passo 2
C) a Mallory não for o atancante D) houver conluio entre o Bob e a Mallory
E) pelo menos um dos dois, o Bob ou a Mallory seja de confiança.

54. Se houver conluio[1] entre o Bob e a Mallory, a Alice:

A) saberá se a mensagem recebida pela Carol foi alterada B) saberá se a mensagem foi lida pelo Bob ou pela Mallory
C) não saberá se a mensagem recebida pela Carol foi alterada D) saberá quem foi que alterou a mensagem
E) só saberá que houve conluio se a mensagem tiver sido alterada.

[1] combinados entre si

Questão 8

O código de Gray é um sistema de código binário inventado por Frank Gray. Neste código, os padrões de bits são escolhidos de modo a que apenas um bit mude entre dois valores sucessivos. Por exemplo, com 3 bits, os valores entre 0 e 7 podem ser representados por: 000, 001, 011, 010, 110, 111, 101, 100.

Suponha que pretende construir um sistema P2P inspirado no código de Gray, com capacidade para N nós, tal que $N = 2^k$, e os identificadores dos nós terão k bits e respeitarão a regra que entre dois identificadores sucessivos apenas muda 1 bit. A topologia da rede formará um hipercubo, onde cada nó será um vértice e estará ligado a todos os nós cujo identificador difere do seu em 1 bit apenas.

Para cada uma das seguintes afirmações indique se é `[V]`erdadeira ou `[F]`alsa. Em caso de dúvida, justifique a resposta no verso da folha de respostas. Respostas erradas descontam.

55. Este sistema P2P deverá ser considerado estruturado basta considerar que a sua topologia forma um hipercubo.
56. Neste sistema, quando completamente povoado, para chegar a qualquer nó, bastará que cada nó conheça 1 outro.
57. Neste sistema, quando completamente povoado, basta ter k vizinhos para que o encaminhamento entre quaisquer 2 nós custe no máximo k passos;
58. Neste sistema, quando completamente povoado, basta ter $log\ k$ vizinhos para que o encaminhamento entre quaisquer 2 nós custe no máximo $log\ k$ passos;
59. Neste sistema, entre 2 quaisquer nós, que não sejam vizinhos diretos, existem vários caminhos óptimos.

Responda em formato livre às seguintes questões no verso da folha de respostas.

60. Apresente um esboço do algoritmo de encaminhamento a usar neste sistema para enviar uma mensagem entre dois nós.
61. Supondo que pretende fazer broadcast de uma mensagem neste sistema, será possível fazê-lo sem que a mesma seja entregue mais do que uma vez no mesmo nó? Justifique.