MIEIC **SISTEMAS DISTRIBUÍDOS – 10/11** **FEUP**

Tipo de prova: com consulta
Duração: 2 horas
Cotação máxima: 20 valores
Estrutura da prova: Parte I (escolha múltipla, 50%); Parte II (teórica, 50%).

Exame da Época Normal
21 de Junho de 2011

Nome:_____
ID:_____

Parte I: Escolha Múltipla [10 valores]

Utilização: para cada pergunta **só há uma** resposta correcta; indique-a fazendo um círculo nesta folha.

Cotação: cada resposta certa vale 1 ponto; cada resposta errada vale -0.3 pontos; cada resposta ambígua, ininteligível ou não assinalada vale 0 pontos. O total são 10 pontos.

1. Um cliente executa um *remote procedure call* (RPC). Apesar de o servidor executar o pedido, este falha ao enviar a resposta. Qual é o comportamento do cliente se o sistema usar a semântica "at most once"?
   a. Continua a sua execução após enviar o pedido
   b. Envia um novo pedido após ocorrer um time-out
   c. Envia novo pedido para confirmar que o anterior foi executado
   d. Fica bloqueado, eventualmente continua após um time-out

2. Um sistema distribuído usa o algoritmo de Berkeley para sincronizar os relógios locais das suas três máquinas. O time-deamon inicia o processo de sincronização às 2:05:00. Se os relógios locais das outras máquinas tiverem os valores 2:04:50 e 2:05:22, qual será o tempo em cada máquina após a sincronização?
   a. 2:05:00; 2:05:00; 2:05:00
   b. 2:05:04; 2:05:04; 2:05:04
   c. 2:05:06; 2:05:06; 2:05:06
   d. 2:05:22; 2:05:22; 2:00:22

3. Qual das seguintes afirmações é verdadeira num sistema que usa o relógio lógico de Lamport (*Lamport Logical Clock*)
   a. Os processos usam o algoritmo de sincronização de Lamport para actualizaram os relógios locais
   b. Os processos incrementam o relógio antes de enviarem um evento, e juntam o valor do relógio em cada mensagem enviada
   c. Os processos incrementam o relógio num intervalo específico e actualizam o valor quando receberem uma mensagem com um tempo maior
   d. Um processo só actualiza o seu relógio quando recebe uma mensagem que tiver um valor maior do que o seu valor

4. Num sistema de ficheiros distribuído, é preferível disponibilizar um modelo de acesso remoto porque
   a. O servidor não é um possível ponto de congestionamento do sistema
   b. Facilita a manutenção da consistência
   c. É possível usar um *mounter* automático para manter a consistência
   d. É possível usar servidores com estado

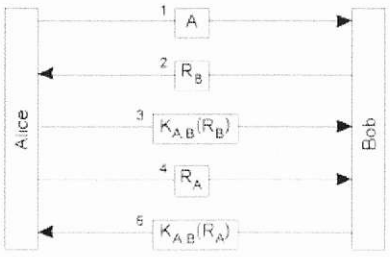
5. *Network file system* (NFS) lida com falhas no RPC usando
   a. *Dynamic Object Invocation*
   b. Cache no servidor e IDs nas transações RPC
   c. Serviços de eventos e notificações
   d. *Asynchronous Method Invocation*

6. O que faz um modelo de falhas ser bizantino
   a. Falhas intermitentes
   b. Comportamento arbitrário após a ocorrência duma falha
   c. A falha resulta num *crash* do sistema
   d. Servidores param de responder após a falha, embora os clientes funcionem normalmente

7. Sobre o Google File System (GFS) discutido nas aulas teóricas, qual a alínea correcta
   a. Os ficheiros são divididos em *chunks* de 64MBytes
   a. *Chunks* são guardados em *chunk servers*
   b. Clientes interagem com o *GFS master* para obter o contacto do *chunk server* que está a partilhar um *chunk*, e com o *chunk server* para ler e/ou escrever num dado *chunk*
   c. Todas as outras alíneas estão correctas

8. Quando estivermos a resolver um nome num dado *namespace*, resolução iteractiva é pior do que recursiva porque
   a. Comunicações entre máquinas que estão longe custam menos
   b. Não consegue usar o sistema de caching do servidor de forma eficiente
   c. Exige mais trabalho nos servidores de nomes
   d. A resolução do nome do cliente é mais simples

9. Considere o seguinte protocolo de autenticação, onde R_A e R_B são identificadores *"once-in-a-lifetime" (nonce)*. Qual das seguintes afirmações é verdadeira?
   a. O protocolo é vulnerável a ataques por reflexão
   b. O protocolo é vulnerável a ataques por repetição de mensagens antigas
   c. O protocolo é baseado em chaves simétricas
   d. O protocolo é vulnerável porque a primeira mensagem não é encriptada.



10. Nas propriedades ACID, qual das seguintes definições não é válida
    a. *Atomic*: se uma transacção não conseguir executar todas as suas operações, algumas das suas operações serão visíveis desde que executadas na respectiva ordem
    b. *Consistent*: as transacções não alteram a integridade da estrutura de dados
    c. *Isolated*: se duas ou mais transacções estão a executar ao mesmo tempo, o resultado final é o mesmo que executar essas transacções sequencialmente
    d. *Durable*: Os efeitos de uma transação em caso de sucesso (*commit*) são permanentes

Parte II: Predominantemente teórica [10 valores]

Utilização: Justificar (brevemente) as suas respostas ; Cotação: indicada em cada pergunta.

1. **[1 val.]** Defina sucintamente o que é um sistemas distribuído, e apresente 4 características fundamentais para o seu bom funcionamento?

2. **[5 val.]** Considere uma aplicação de transferência de ficheiros que permite que um cliente transfira ficheiros de e para o servidor
   a. Enumere e descreva sinteticamente três operações básicas que deverão ser suportadas por esse serviço. Para cada uma das operações especifique os seus argumentos e valores de retorno.
   b. Admita que teria que implementar uma aplicação deste tipo usando a pilha protocolar da Internet. Que protocolo de transporte considera mais adequado? Justifique.
   c. Uma alternativa a uma implementação usando directamente os protocolos de transporte da Internet seria usar um serviço de comunicação assíncrona. Enuncie a principal vantagem e a principal desvantagem de uma implementação deste tipo.
   d. Suponha que pretendia fornecer um serviço de acesso a informação eficiente e robusto. Que tipo de sistema de ficheiros distribuídos recomendaria para o servidor? Justifique constrastando com outras soluções para o sistema de ficheiros.
   e. Considere concorrência do lado do servidor. Explique a sua principal vantagem e como poderia ser implementada para concretizar essa vantagem. Descreva quaisquer riscos de race conditions na implementação que propõe.
   f. Admita que se pretende implementar controlo de acesso. Uma possibilidade para autenticar os utilizadores é o uso de um par (*username, password*). Descreva **um** potencial problema de segurança desta alternativa, e como poderia ser resolvido.
   g. Identifique 1 possível "falha" no servidor. Explique as suas consequências e como poderia minorar essas consequências (**Sugestão**: aborde a consistência e replicação dos dados).

3. **[2 val.]** Sobre sistemas de nomes
   a. Explique a conveniência de serviços de nomes em sistemas distribuídos.
   b. Dada a sua estrutura, os nomes podem ser de um de dois tipos. Descreva-os.
   c. Admita que o domínio *fa.up.pt* não é uma zona, mas antes está integrado na zona de *up.pt*. Descreva o processo de resolução do nome *www.fa.up.pt* a partir de um computador ligado ao subdomínio *eslab.upc.edu*, admitindo que este é uma zona. Assuma ainda que o registo A associado a *www.fa.up.pt* não se encontra em possíveis caches. (**Sugestão**: Faça uma figura)

4. **[2 val.]** Sobre *Distributed Hash Tables*
   a. Usando o algorimo Chord, apresente as *finger tables* dos nós 0, 1, 2, e 6 (**Sugestão**: Faça uma figura). Assuma um espaço de endereços de identificação entre 0 e 8 e que só estes nós estão ligados na rede.
   b. Sabendo que o nó 0 tem o item 7 e o nó 1 o item 1, quais os nós visitados até encontrar o item 7 a partir do nó 1?
   c. Apresente **duas** vantagens e **uma** devantagem do protocolo Chord.

pMIEIC **SISTEMAS DISTRIBUÍDOS – 10/11** **FEUP**

Tipo de prova: com consulta
Duração: 2 horas
Cotação máxima: 20 valores
Estrutura da prova: Parte I (escolha múltipla, 50%); Parte II (teórica, 50%).

Exame de Recurso
14 de Julho de 2011

Nome:_____
ID:_____

Parte I: Escolha Múltipla [10 valores]

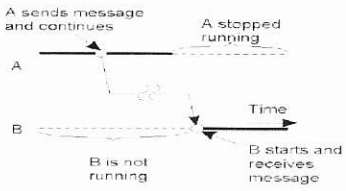
Utilização: para cada pergunta **só há uma** resposta correcta; indique-a fazendo um círculo nesta folha.

Cotação: cada resposta certa vale 1 ponto; cada resposta errada vale -0.3 pontos; cada resposta ambígua, ininteligível ou não assinalada vale 0 pontos. O total são 10 pontos.

1. Um cliente executa um *remote procedure call* (RPC). Apesar de o servidor executar o pedido, este falha ao enviar a resposta. Qual é o comportamento do cliente se o sistema usar a semântica "*exactly once*"?
   a. Continua a sua execução após enviar o pedido
   b. Envio um novo pedido após ocorrer um time-out
   c. Envio novo pedido para confirmar que o anterior foi executado
   d. Fica bloqueado, eventualmente continua após um time-out

2. O algoritmo de Berkley pode ser considerado um
   a. Algoritmo de sincronização centralizado
   b. Algoritmo de sincronização distribuído
   c. Algoritmo centralizado para sincronização de relógios lógicos
   d. Algoritmo distribuído para sincronização de relógios lógicos

3. Considere a seguinte comunicação
   1 - A quer enviar uma mensagem para B
   2 - B não está disponível e *A continua a sua execução*
   3 - B fica entretanto disponível
   4 - A envia a mensagem e continua a execução
   5 - B recebe a mensagem

   Que tipo de comunicação é descrita neste exemplo?
   a. *Transient asynchronous communication*
   b. *Transient synchronous communication*
   c. *Persistent asynchronous communication*
   d. *Persistent synchronous communication*

4. Num sistema de ficheiros distribuído, é preferível disponibilizar um modelo Upload/Download porque
   a. O servidor não é um possível ponto de congestionamento do sistema
   b. Facilita a manutenção da consistência
   c. É possível usar um *mounter* automático para manter a consistência
   d. É possível usar servidores com estado

5. Sobre operações idempotentes
    a. Acrescentar informação num ficheiro é uma operação idempotente
    b. Adicionar um número diferente de zero numa conta bancária não é uma operação idempotente
    c. Adicionar um elemento a uma *queue* não é uma operação idempotente
    d. Nenhuma das respostas anteriores

6. Suponha que um sistema *crasha* 1 vez por mês, demorando 10 minutos a fazer o reboot.
    a. O *Mean Time to Failure* desse sistema é igual a 10 horas
    b. O *Mean Time to Revovery* é igual a 720 minutos
    c. O sistema apresenta uma taxa de disponibilidade de 99.9%
    d. O sistema apresenta uma taxa de indisponibilidade de 0.3%

7. Sobre exclusão mútua distribuída
    a. É resolvida usando mensagens, assumindo uma rede fidedigna, assíncrona e que os processos podem falhar
    b. É resolvida trocando mensagens entre os intervenientes, assumindo uma rede fidedigna e síncrona
    c. Poder ser resolvida mantendo estado partilhado (e.g., *atomic test-and-set* de uma variável partilhada)
    d. Todas as outras alíneas estão correctas

8. Em exclusão mútua, qual das seguintes é uma vantagem do modelo *central server* (servidor central) para garantir exclusão mútua
    a. É um modelo simples que só necessita de 3 mensagens por *entry/exit*
    b. Tem de eleger um servidor central
    c. Só existe um ponto de falha no sistema, o próprio *central server*
    d. O *central server* é o único ponto de congestionamento na rede.

9. Sobre o modelo *2-Phase Commit*
    a. Antes de fazer um *commit*, requer uma fase de *pre-commit*
    b. Se o coordenador e um participante crasharem o sistem pode bloquear até pelo menos um deles voltar a estar activo
    c. Não é usado na prática em detrimento da 3-*Phase Commit*
    d. O coordenador consegue juntar-se rapidamente e sem qualquer input externo após um crash

10. Sobre a ordem casual de Lamport, ou seja, a ordem *happens-before* (->)
    a. Se o evento x e y ocorrem nos processos P1 e P2 respectivamente, então ou x->y ou y->x
    b. O relógio lógico baseado na ordem de Lamport está directamente relacionado com o valor do relógio físico da máquina
    c. *Totally ordered logical clocks* baseados na ordem de Lamport são obtidos se, por exemplo, considerarmos o *id* do processo
    d. Nenhuma das repostas anteriores

Parte II: Predominantemente teórica [10 valores]

Utilização: Justificar (brevemente) as suas respostas ; Cotação: indicada em cada pergunta.

1. **[4 val.]** Em sistemas de ficheiros distribuidos
   a. Descreva sucintamente o que são servidores **sem estado** e enumere 3 vantagens em oferecer esse serviço?
   b. Descreva sucintamente o que são servidores **com estado** e enumere 3 vantagens em oferecer esse serviço?

2. **[3 val.]** Sobre Consenso
   a. Descreva sucintamente o funcionamento do algoritmo Paxos (divida a sua discrição em 4 fases fundamentais).
   b. Qual a relação entre o algoritmo Paxos e os relógios lógicos de Lamport?
   c. Descreva uma situação onde o algoritmo Paxos ajude a resolver um problema de replicação.
   d. Demonstre que, mesmo na presença de um canal fidedigno, 3 processos nunca conseguirão chegar a um consenso se pelo menos um dele exibir um comportamento bizantino.

3. **[2 val.]** Considere um cenário em que se utiliza criptografia simétrica e um centro de distribuição de chaves secretas de sessão como o pressuposto pelo algoritmo de Needham-Schroeder para criptografia simétrica. Suponha ainda que o centro de distribuição de chaves já conhece as chaves secretas de todos os elementos envolvidos. Apresente um protocolo através do qual um elemento pode mudar a sua chave secreta guardada pelo servidor de chaves. A sua solução deverá resistir a todas as formas de ataque mais conhecidas incluindo "replaying" e "masquerading". Como é evidente nenhuma das chaves (a velha e a nova) deverão passar "em claro" na rede. Deverá explicitar todos os pressupostos e argumentar sobre a correcção da sua solução.

4. **[1 val.]** Descreva a forma como geralmente é gerida a *cache* de ficheiros nos clientes NFS com o objectivo de aumentar o desempenho e diminuir a probabilidade de se violar a semântica da partilha concorrente de ficheiros.