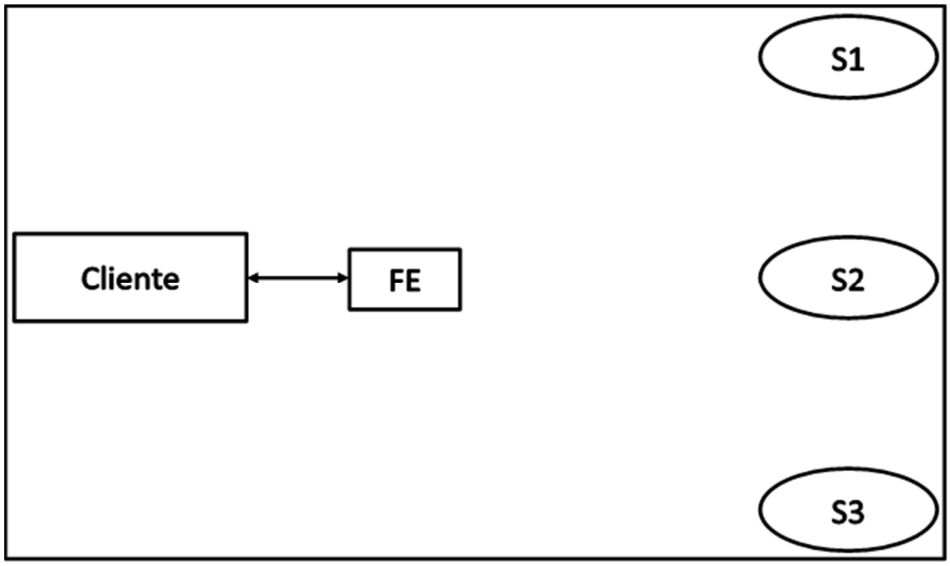
LEIC/LERC – 2012/13, 2º Teste de Sistemas Distribuídos, 5 de Junho de 2013

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 1h30m

Grupo I [12v]

1) Considere um sistema replicado em que um cliente (C) interactua através de um Front-End (FE) com um conjunto de três servidores (S1, S2, S3). As operações sobre os servidores são apenas de leitura (R) e escrita (W). O protocolo usado é o de p*rimary-backup.* Assuma que os servidores são de **falha silenciosa**, que o sistema é síncrono, que a rede não tem falhas permanentes e garante uma ordem FIFO das mensagens.

   a) [0,9v] Considere que o cliente efectua uma escrita na variável A (W(A,10)) e depois lê o valor da mesma variável R(A). Complete o diagrama indicando as operações que são realizadas, descrevendo-as através de setas com a legenda das operações (W(A, 10), R(A)). Escreva as legendas que achar necessárias, indique todas as mensagens trocadas entre cliente e os servidores, e entre estes.



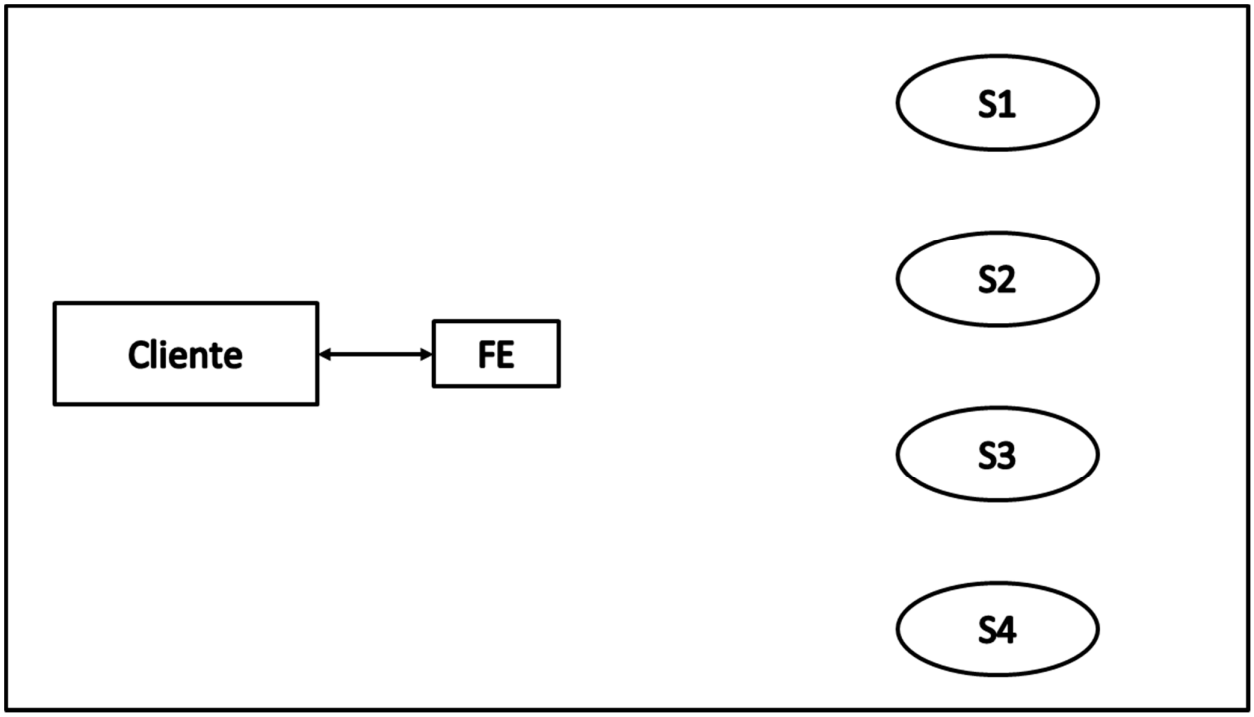
   b) [0,6v] Explique quantas falhas de servidores pode tolerar este sistema. Justifique.

   c) [0,8v] Escreva uma expressão que calcule o tempo máximo de indisponibilidade de sistema, considerando que o cliente utiliza um servidor de nomes (tipo UDDI) para conhecer o endereço do servidor? Defina todos parâmetros os presentes na expressão (ex.: t_reg_uddi - tempo de registo no UDDI, etc.)

2) Considere agora que a **rede é assíncrona** e que utiliza um protocolo de quórum de maioria.

a) [0,9v] O que significa o pressuposto que o sistema é assíncrono e o que muda em relação ao sistema da pergunta 1?

b) [1,1v] Pressupondo que executa a operação (W(A, 10), R(A)). Complete o diagrama com todas as interacções entre o cliente e os servidores, admitindo que S2 não recebe a mensagem de write e S3 falha depois aquando da execução de R(A).



c) [0,6v] Quantas falhas silenciosas dos servidores tolera este sistema? Justifique.

d) Considere que o servidor S1 está ligado a um *backbone* de rede com elevada banda passante, e os restantes têm ligações idênticas e mais lentas à rede (para exemplo a ligação é 3 vezes mais rápida). Como poderia optimizar o funcionamento do sistema para acelerar as estruturas, passando a usar um **protocolo de quóruns com pesos variáveis**?

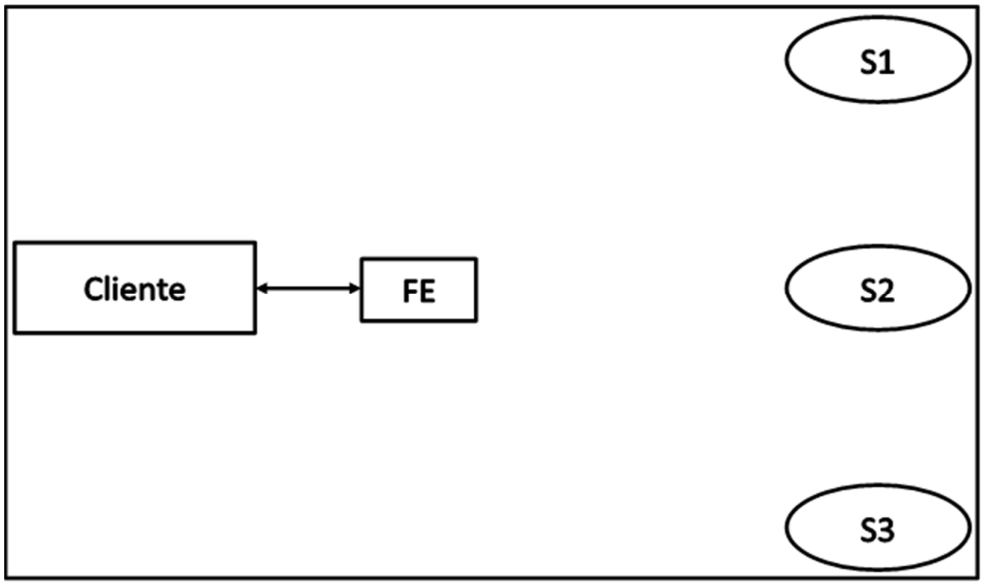
i) [1,1v] Explique como definiria os pesos de cada servidor e os valores RT e WT

ii) [0,9v] Justifique com um exemplo qual a melhoria que esta proposta apresenta em relação ao quórum de maioria.

3) [0,9v] Considere agora que os servidores são de **falha arbitrária**. Em que difere este tipo de falha da falha silenciosa? Apresente um exemplo para o cenário da pergunta 1.

4) Mantendo a configuração da alínea 1), mas pressupondo outra aplicação em que o cliente quer executar sobre os 3 servidores operações de leitura e escrita sobre **dados diferentes** e garantindo transacções atómicas distribuídas, usando 2-phase commit (2PC).

a) [0,6v] Adicione ao diagrama seguinte um componente indispensável para poder executar as transacções distribuídas.



b) [0,6v] Represente no diagrama acima, através de setas, todas as interacções que desencadeia a execução da operação *openTransaction.*

c) [0,6v] Represente no diagrama acima, através de setas, todas as interacções que desencadeia a execução da transação distribuída composta pela escrita da variável X no servidor S1 e pela leitura da variável Y no servidor S2. Considere só a representação até esse momento; a evolução subsequente e em particular o 2PC não fazem parte desta representação.

d) [0,9v] Depois desta operação o servidor S1 falha.

i) Como será detectado?

ii) O que irá suceder à transacção global nesse caso?

e) [0,6v] Considere agora uma execução alternativa em que a transacção decorre normalmente até ao cliente fazer closeTransaction e o servidor S1 falha depois de ter respondido ao *canCommmit* (*prepare)* com *yes* (*ready)*. O que irá suceder à transacção global? Justifique.

f) [0,9v] Considere agora uma execução alternativa em que a transacção decorre normalmente até ao cliente fazer closeTransaction e o servidor S1 falha depois de ter efectuado o *commit* local mas antes do *acknowledge* ao coordenador.

i) Como será detectado?

ii) O que irá suceder à transacção global?

Grupo II [8v]

1) Considere dois interlocutores, A e B.

Assuma que, após distribuição através de um canal seguro, A conhece a sua chave privada, KsA, e a chave pública de B, KpB; e vice-versa.

Por vezes, A e B pretendem trocar múltiplas mensagens entre si e para tal seguem o seguinte protocolo:

- O nó (A ou B) que tomar a iniciativa primeiro, gera uma chave simétrica secreta, K.
- Se for o nó A que gerou a chave K, A envia {K}KpB a B; B decifra com KsB e obtém K. (Procedimento inverso para o caso em que B toma primeiro a iniciativa.)
- Sempre que A queira enviar mensagem M a B, ou vice-versa, é enviado {M}K pela rede.

Nas alíneas seguintes assuma que o atacante não consegue quebrar as chaves secretas (KsA, KsB e K).

a) [0,6v] Quando A quer enviar M a B, A poderia optar pela alternativa de enviar {M}KpB. Que desvantagens encontra nesta solução, comparativamente à solução descrita acima?

b) O protocolo indicado na alínea 1) é passível de ataque *man in the middle*, em que um intruso T consegue levar A e B a trocarem mensagens cifradas sem saberem que T consegue ter acesso ao respectivo conteúdo em claro.

   i) [1,0v] Descreva o procedimento que T deverá levar a cabo para concretizar este ataque. Ilustre com um exemplo.

   ii) [1,0v] Proponha uma correcção ao protocolo descrito acima que previna este ataque.

c) O protocolo na alínea 1) é também vulnerável a ataques de repetição (*replay*).

   i) [0,8v] Descreva de que forma um atacante T pode concretizar esse ataque. Ilustre com um exemplo em que B é um servidor de contas bancárias e permite aos clientes debitarem/creditarem as suas contas.

ii) [1,0v] Proponha uma correcção ao protocolo que previna este ataque.

2) Para cada mensagem M recebida por A ou B, o receptor pretende ter forma de garantir confidencialidade, integridade e não repúdio da mensagem.
   a) [0,9v] Apresente detalhadamente uma solução que garanta esses 3 requisitos.

   b) [0,9v] Apresente agora uma solução mais eficiente que não ofereça a garantia de não repúdio.

3) Uma forma de A ter tomado conhecimento da chave pública de B foi através de um certificado digital de chave pública X509.
   a) [0,9v] Indique os campos principais de um certificado X509 e respectivo significado.

   b) [0,9v] A obteve o certificado da chave pública de B a partir de um site desconhecido na Web. Pode A confiar na chave que vem no certificado? Se sim, que passos deve A efectuar para confirmar que a chave é realmente a chave pública actual de B? Se não, justifique.