LETI 2019/20, Repescagem do 2º Teste de Sistemas Distribuídos
31 de janeiro de 2020

Identifique todas as folhas. Responda no enunciado, usando apenas o espaço fornecido.

Nas perguntas de escolha múltipla assinaladas com EM existe apenas uma resposta certa.
Uma resposta errada desconta 1/(N-1) do valor de uma pergunta com N opções de resposta.

Duração da prova: **1h15m**

Grupo I [3 valores]

1) [0,6v] Associe o conceito à sua definição:

Erro	●	● Transição do sistema para um estado interno incorreto.
Falta	●	● Desvio do comportamento observado em relação ao comportamento especificado.
Falha	●	● Acontecimento que altera o padrão normal de funcionamento de um componente do sistema.

2) Considere o contexto de um **servidor web** que suporta uma loja eletrónica.

a) [0,8v] Dê um exemplo de uma falta **humana** e **não determinística**. Justifique.

b) O servidor web deveria operar corretamente durante um período de 1000 minutos. Durante este período, ocorreram 2 falhas. O tempo de reparação de todas as falhas totalizou 10 minutos.

i) [0,8v] Calcule a **disponibilidade** do sistema.

ii) [0,8v] Se reduzirmos o **MTTR**, isso vai melhorar ou piorar a disponibilidade do sistema? Justifique.

Grupo II [9 valores]

1) Considere um sistema replicado que segue um protocolo baseado no ***primary-backup***, mas com um **servidor de nomes** que permite localizar as diferentes réplicas. O *front-end* resolve sempre o nome do servidor antes de o contatar através da função resolve que devolve o endereço na rede de uma réplica.

   Registaram-se as seguintes mensagens:

   - C -> FE read(a)
   - R1 -> R2 …
   - FE -> NS resolve(S)
   - NS -> FE addressOf(R1)
   - FE -> R1 read(a)
   - R1 -> FE a=100
   - R1 -> R2 …
   - FE -> C a=100

   C – cliente; FE – front-end; S – serviço; R1 – réplica primária; R2 – réplica secundária; NS – servidor nomes. *a* é uma variável inteira.

   a) [0,6v] Qual é o conteúdo e propósito das mensagens periódicas R1 -> R2 … ?

   b) [0,7v] Antes da resposta ao cliente, não deveria ter surgido R1 -> R2 read(x)?
   Considera este comportamento normal ou uma falta? Justifique.

   c) [1,0v] O cliente pretende agora executar ***write(a, 300)***.
   Complete uma possível sequência de mensagens sendo que R1 KO representa a falta silenciosa de R1.
   Complete a sequência até que o sistema recupere da falta (caso recupere). Pode adicionar mais ●

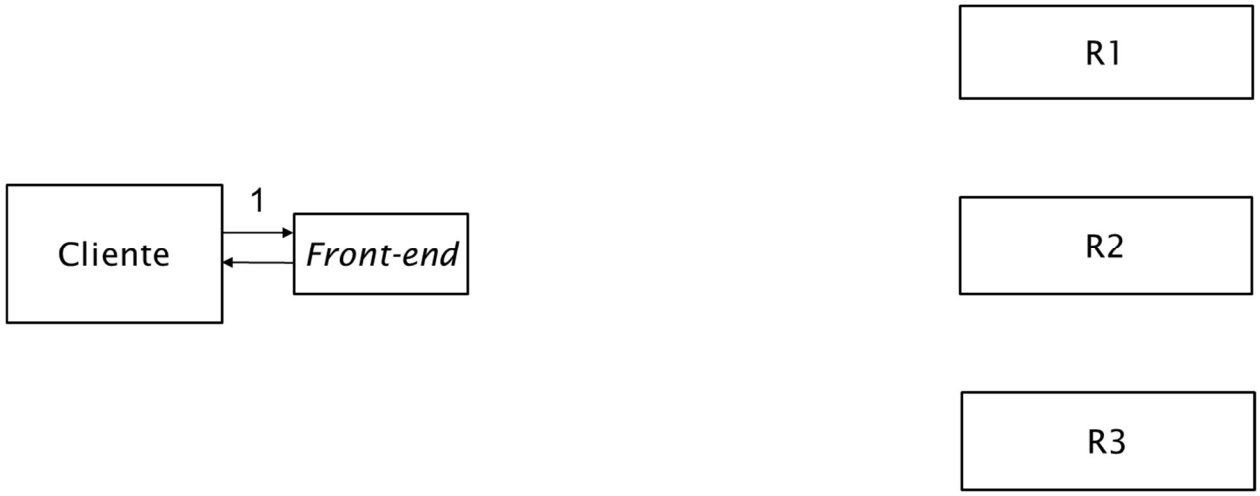
   - C -> FE write(a, 300)
   - FE -> NS resolve(S)
   - NS -> FE addressOf(R1)
   - FE -> R1 write(a, 300)
   - **R1 KO**
   -
   -
   -
   -
   -
   -

d) [0,7v] Qual é o cálculo correto para o tempo de recuperação do serviço assumindo *primary-back com naming server*?

A. (P + tmax) + (tpublishNS + tresolveNS) + tretryFE
B. P + tpublishNS + tretryFE
C. (P + tmax) + tpublishNS + tretryFE + tresponse
D. (P + 3*tmax) + (tpublishNS + tresolveNS) + tretryFE

2) Considere agora outro sistema replicado, em que o protocolo usado é o ***quorum consensus*** e o sistema é assíncrono. O valor inicial da variável inteira *b* é 0.

a) [1,4v] Considere que o cliente quer executar a operação *write(b, 20)*.
Complete o diagrama com todas as **mensagens numeradas** e respetiva **legenda** com toda a informação.
Considere que R1 está "em baixo" (não responde) quando a mensagem de escrita lhe é dirigida.



1 – O cliente envia *write(b,20)* para o FE (*Front-End*)

2 –

b) [0,8v] Considere agora uma operação *read(b)* que se executa posteriormente à escrita anterior.
R1 está agora "em cima", mas R3 está "em baixo".
A leitura vai devolver 0 ou 20 ao cliente? Justifique, em detalhe, de que forma é feita escolha.

c) [0,8v] No *quorum consensus* é possível definir diferentes limiares para as leituras e para as escritas.
Em que situações se justifica fazer essa configuração? Dê um exemplo.

3) Considere agora que o protocolo usado é o ***gossip*** estudado nas aulas, e que o sistema é assíncrono.

Pretende-se usar um servidor para registar os **acessos a um edifício**, feitos com utentes, com um cartão pessoal. Cada entrada do edifício – **N**orte, **S**ul, **E**ste, **O**este – tem uma réplica de servidor onde são registados os acessos. Vamos designar as réplicas por RN, RS, RE, RO.
Em cada entrada existe um cliente, que vamos designar por CN, CS, CE, CO.
Cada vez que há uma entrada ou uma saída, o cliente envia um registo para um servidor. O cliente tem preferência pelo servidor mais próximo – CN prefere RN, CS prefere RS, e assim sucessivamente – mas pode também contactar outros servidores, se necessário.

O objetivo inicial da aplicação é calcular estatísticas de utilização do edifício, por exemplo, perceber quais são as entradas mais usadas e quando.

Considere a seguinte sequência que foi executada:
João e Catarina entram na porta sul, CS -> RS
Pedro, Ana e Francisco entram na porta este, CE -> RE
Guilherme entra na porta norte, CN->RN

a) EM [0,6v] Quantas faltas de servidores podem ser toleradas por este sistema?
A. zero B. uma C. duas D. três

b) [0,4v] Indique o *timestamp* vetorial de cada réplica, após a sequência executada e assumindo que não houve ainda nenhuma ronda de *gossip*.

TS_RN =
TS_RS =
TS_RE =
TS_RO =

c) [0,5v] Descreva, por palavras, o que deverá acontecer quando o RN faz *gossip* com o RS.

d) [0,4v] Indique o *timestamp* vetorial de cada réplica, após o *gossip* entre RN e RS.

TS_RN =
TS_RS =
TS_RE =
TS_RO =

e) [0,6v] Qual deverá ser o procedimento para verificar, com determinismo, se um dado utente está ou não dentro do edifício? Descreva e justifique os passos do algoritmo.

f) [0,5v] A solução descrita na alínea anterior é tolerante a partições de rede? Por exemplo, imagine que deixa de ser possível a RN e RO contactar com RS e RE. Justifique.

Grupo III [8 valores]

1) O TLS (*Transport Layer Security*), que está na base do HTTP**S**, permite estabelecer um canal seguro entre clientes e servidores ligados à Internet. Quando um cliente inicia uma nova ligação com um servidor que não conhece e com o qual não partilha nenhum segredo, o servidor envia-lhe um certificado digital.

   a) [1,2v] Desenhe um diagrama com o conteúdo do certificado digital, usando como referência a norma X.509. Faça uma legenda para explicar o significado de cada parte.

   b) [1,0v] Descreva todos os passos do procedimento que deve ser seguido pelo cliente para verificar o certificado digital.

   c) [1,0v] Se um intercetor – *man-in-the-middle* – trocar o certificado do servidor por um falso certificado logo na primeira interação entre o cliente e o servidor, é possível ao cliente detetar esse ataque? Justifique.

   d) [0,8v] Proponha algoritmos criptográficos concretos a ser usados para a verificação de assinatura. Descreva qual a entrada (*input*) e saída (*output*) de cada algoritmo.

Algoritmo 1:
Algoritmo 2:

2) Considere o caso de uma empresa portuguesa que comprou uma solução de correio eletrónico seguro e que a vai pôr em utilização para toda a comunicação interna entre colaboradores. O manual técnico da solução afirma o seguinte:

"O título da mensagem não é cifrado, mas é enviado com um resumo SHA-2."

"O corpo da mensagem é cifrado com AES de 256 bits, em modo ECB,
usando como chave um segredo partilhado entre um emissor e o recetor da mensagem.
Cada segredo deve ser configurado previamente na aplicação de correio eletrónico."

a) [0,4v] O 256 do AES refere-se ao número de bits da chave ou ao tamanho do bloco?

b) [0,8v] O modo ECB introduz alguma vulnerabilidade na cifra? Justifique.

c) Assumindo que a descrição acima é completa, que propriedades de segurança são garantidas…
   i) [0,8v] … para o título da mensagem? Justifique.

   ii) [0,8v] … para o corpo da mensagem? Justifique.

d) [1,2v] Suponha agora que o presidente da empresa vai usar o sistema para enviar uma mensagem para todos os 1230 colaboradores.
   Proponha uma alteração ao protocolo que, mantendo as propriedades de segurança, envie a mensagem para todos os destinatários sem ter que cifrar o corpo da mensagem 1230 vezes.
   Desenhe um diagrama para a sua resposta com uma legenda explicativa.