

**DI/FCT/UNL**  
**Mestrado Integrado em Engenharia Informática**

**Confiabilidade de Sistemas Distribuídos**  
**2º Semestre, 2015/2016**

**Teste de Avaliação nº 1 (22/Abril/2017)**  
**Componente: Teste da Parte Prática**

Considere a sua solução de replicação do sistema DDS (*Dependable Storage System*) que desenvolveu no trabalho prático nº 1. Caracterize a sua solução indicando X nas respetivas células (cinzentas) da seguinte tabela. Caso seja necessário pode consultar ou testar a sua implementação no caso de necessitar para responder a alguma ou algumas das questões.

<b>Solução de replicação utilizada</b>	
1) Modelo de quórum com tolerância a falhas ou ataques bizantinos	
2) Modelo de replicação de máquina de estados com base numa implementação baseada no algoritmo PAXOS	
<b>Ambiente de programação usado e linguagem de programação adotada</b>	
3) Java (indique a versão)	
4) Akka, com programação em Java	
5) Akka, com programação em Scala	
7) Solução híbrida: indique como caracteriza:	
<b>Interação entre o cliente e o repositório é suportada em:</b>	
8) Sockets TLS, com autenticação mútua cliente/servidor	
9) Sockets TLS, com autenticação do servidor	
10) REST/TLS, com autenticação mútua cliente/servidor	
11) REST/TLS, com autenticação do servidor	
12) Qual a suite criptográfica utilizada no estabelecimento (handshake) da sessão TLS e que algoritmo criptográfico simétrico suporta a sessão TLS ?  Handshake e autenticação:  Algoritmo criptográfico que cifra as mensagens no canal TLS:	
<b>Interação entre as réplicas</b>	
13) Sockets TLS, com autenticação mútua cliente/servidor	
14) Sockets TLS, com autenticação do servidor	
15) REST/TLS, com autenticação mútua cliente/servidor	
16) REST/TLS, com autenticação do servidor	

17) Outra solução. Indique qual.	
18) Qual a suite criptográfica utilizada no estabelecimento (handshake) da sessão TLS e que algoritmo criptográfico simétrico suporta a sessão TLS na comunicação segura entre as réplicas?  Handshake e autenticação:  Algoritmo criptográfico que cifra as mensagens no canal TLS:	

Realização dos objetivos do trabalho (indique S – Sim, N – Não e P – Parcialmente Justifique abaixo a escolha nos casos indicados com P			
Requisito	S	N	P
19) Todas as funções da API para o cliente (referida como API primária) foram totalmente implementadas, de acordo com a especificação do enunciado			
20) Todas as funções da API para o cliente (referida como API primária) foram totalmente testadas, funcionando corretamente			
21) Foi concluída a avaliação experimental de acordo com todos os critérios pedidos ( <i>benchmarks</i> 1 a 5), mas não foram testadas injeção de falhas por crash nem falhas bizantinas			
22) Foi concluída a avaliação experimental de acordo com todos os critérios pedidos, ( <i>benchmarks</i> 1 a 5), mas apenas se testou com injeção de falhas por crash			
23) Foi concluída a avaliação experimental de acordo com todos os critérios pedidos, ( <i>benchmarks</i> 1 a 5) tendo sido testadas falhas por crash e falhas bizantinas			

### Questão 1

- Indique na sua implementação onde e em que condições as propriedades de *safety* e *liveness* são satisfeitas e em que condições as mesmas são satisfeitas.
- Quais as operações da API providenciada para o cliente têm pior latência ? Indique se isso seria expectável e justifique porquê.
- Argumente porque é que o seu sistema de replicação funciona corretamente descrevendo a avaliação de comprovação experimental que lhe permite estar certo disso.

### Questão 2

De acordo com a sua implementação responda a uma apenas das seguintes alíneas:

- Explique como procedeu à integração do sistema BFTsmart na sua solução.
- Explique como forma os quóruns de escrita e de leitura na implementação que realizou.