

Grupo 52

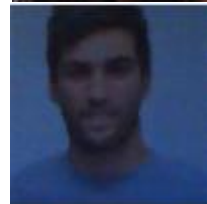
Rodrigo Amaral Cabral Vieira (70315)



Maria Teresa Cardoso dos Santos Coelho (75453)



João Francisco Vieira Gonçalves (76547)



Store-A:

Esta funcionalidade foi totalmente implementada, salvo alguns detalhes. O protocolo implementado foi o Quorum Consensus, de leituras com writeback, readthreshold e writethreshold, e chamadas assíncronas.

As operações de read (load) e de escrita (store) estão totalmente realizadas com o protocolo acima descrito, exceptuando apenas o facto de ser omitida a informação relativamente ao peso de cada servidor. Uma vez que não encontrámos razões suficientes para atribuir mais ou menos peso a um ou mais servidores, considerámos que todos teriam o mesmo, e, portanto, omitimos esse detalhe de implementação.

De forma a assegurar transparência de replicação, foi criada a classe FrontEnd, e, de modo a otimizar o desempenho da resposta ao cliente, foram implementadas invocações assíncronas.

Tal como pedido, também foi garantida a consistência sequencial ao nível de cada documento individual, sendo este requisito testado ao longo de todo o desenvolvimento.

A verificação do limite de capacidade do repositório foi desativada tal como era suposto.

Dito isto, ficaram por realizar:

- cid, pois a tag é apenas composta por nseq, isto porque cada cliente apenas pode aceder aos seus ficheiros;
- pesos distintos para as réplicas, por opção de implementação (como foi acima referido).

ID-B:

Para esta funcionalidade, procurámos garantir a privacidade dos dados enviados na operação store, cifrando-os antes da invocação, e o mesmo para a operação load. Desta forma recorreremos ao algoritmos de hash para resumo SHA-1, que resume os conteúdos a serem guardados (store) ou recebidos (load).

Posteriormente este resumo é encriptado recorrendo ao algoritmo de cifra simétrica AES com BlockCipher CBC e sem padding de modo a garantir a integridade, confiabilidade e autenticidade das operações.

O resumo é passado no cabeçalho da mensagem SOAP e o conteúdo original (texto) é passado no SOAPBody. Desta forma, o servidor consegue assegurar que a mensagem não foi modificada.

Dito isto, ficaram por realizar:

- Decifra do lado do servidor;