

Computação Distribuída [Engenharia Informática] - 2022

[Painel do utilizador](#) / [Disciplinas](#) / [ULHT](#) / [Ano Letivo 2022/2023](#) / [Computação Distribuída-7348 \[Engenharia Informática\]-22](#) / [Geral](#)
/ [Frequência 1ª Época](#)

Iniciada quarta, 18 de janeiro de 2023 às 18:30

Estado Terminada

Terminada quarta, 18 de janeiro de 2023 às 19:46

Tempo gasto 1 hora 16 minutos

Nota Por avaliar

Pergunta **1**

Respondida

Nota: 10,00

Porque é necessário converter as mensagens com um protocolo de representação de dados ? O que pode acontecer se ele não for utilizado ?

É necessário utilizar a representação de dados independente das plataformas para que seja aceite uma transmissão dos dados, se isso não acontecer pode haver perda de informação pois os protocolos agem de forma diferente.

Pergunta **2**

Respondida

Nota: 10,00

Quais são os problemas que se pretendem resolver com os Web Services e porque razão o Sun [RPC](#) e o Java RMI não são adequados para resolver esses problemas ?

Pois ao utilizar o JAVA RMI ou o Sun [RPC](#) teríamos que garantir que toda a gente está a utilizar o java e ainda assim que seja a mesma versão do java para garantir que o formato da mensagem seja exatamente o mesmo. Ou seja, todos os clientes teriam de usar elementos de tecnologias sincronizadas umas com as outras o que cria uma dependência muito grande. A proposta dos Web Services é não depender de apenas um linguagem mais ter a capacidade de lidar com qualquer linguagem de programação.

Pergunta **3**

Respondida

Nota: 10,00

Considere 2 agentes, A e B, uma autoridade de certificação S, e as 4 mensagens do protocolo Needham - Schroeder de autenticação com chave secreta:

1. $A \rightarrow S: A, B, Na$
2. $S \rightarrow A: \{Na, B, Kab, \{Ts, A, Kab\}Kb\}Ka$
3. $A \rightarrow B: \{A, Ta\}Kab, \{Kab, A, Ts\}Kb$
4. $B \rightarrow A: \{Ta + 1\}Kab$

Na mensagem 3, como é que B obtém a chave Kab ? Como é que tem a certeza que a chave é válida ?

A envia a B uma mensagem cifrada com a chave Kab contendo o seu id A, um carimbo Ta e o bilhete que recebeu de S então B decifra o bilhete com a sua chave secreta e tem a chave Kab. Confia no bilhete porque está cifrado com a sua chave secreta e Ts garante que é recente. Usando Kab decifra a outra parte da mensagem, obtém o id A e Ta por isso B confia no id de A pois recebeu essa informação cifrada com uma chave Kab que só pode ter sido gerada por S, que conhece a chave secreta de B.

Pergunta **4**

Respondida

Nota: 10,00

Considere 2 agentes, A e B, cada um com o seu par de chaves pública e privada, respetivamente:

A: KAPub, KAPriv B: KBPub, KBPriv

Considere que A quer enviar a B a mensagem M com **privacidade e autenticação**. Represente a mensagem que A deve enviar a B e descreva porque é que a mensagem garante privacidade e autenticação.

Para combinar privacidade e autenticação primeiro autentico a mensagem assinando com a chave privada de A e depois se eu quiser que ela seja privada eu cifro com a chave privada de B e é essa mensagem que envio pela rede. E do outro lado vou receber essa mensagem e decifrar com ordem inversa primeiro decifro com a chave privada de B e depois decifro com chave publica de A.

Pergunta **5**

Respondida

Nota: 10,00

Se o Coordenador falhar, e quando recuperar verificar que está no estado “Esperar” (ainda não recebeu todos os votos), o que deve fazer para continuar o protocolo Two-Phase Commit ?

Utilizando o protocolo o Two-Phase Commit no estado esperar e se coordenador falhar, ele não pode terminar a transação pois tem que receber a confirmação de todos os participantes além disso pode-se repetir a mensagem global previamente enviada.

Pergunta **6**

Respondida

Nota: 10,00 em 10,00

Estabeleça a correspondência entre as definições e os requisitos dos Sistemas Distribuídos apresentados.

A capacidade de manter o nível de resposta constante face a aumentos significativos do número de componentes, utilizadores ou área de abrangência

Escalabilidade

A capacidade de esconder do utilizador e das aplicações a natureza distribuída do sistema

Transparência

A capacidade de permitir a coerência de vários fluxos de execução realizando acessos simultâneos a recursos partilhados

Concorrência

A capacidade para suportar extensões e interações com outros sistemas sem necessidade de alterar os seus conceitos fundamentais

Abertura

A capacidade para acomodar a variedade, a mudança e a diferença

Heterogeneidade

Pergunta **7**

Respondida

Nota: 10,00 em 10,00

Estabeleça as relações corretas entre as seguintes afirmações sobre as arquiteturas de sistemas distribuídos:

O cliente comunica com um servidor, que por sua vez comunica com outros servidores para satisfazer o pedido e responde ao cliente

Arquitetura cliente-servidor com servidores recursivos

O cliente comunica com um servidor que mantém uma cópia local das respostas recentes e lhe devolve imediatamente a resposta se ela existir na cópia local

Arquitetura cliente-servidor com proxy

O cliente comunica com um servidor que responde a parte do serviço e indica ao cliente outro servidor que este deve contactar para continuar o serviço

Arquitetura cliente-servidor com servidores iterativos

A aplicação tem uma camada de apresentação, uma camada de lógica de negócio e uma camada de dados

Arquitetura de 3 níveis

Os clientes comunicam com outros clientes

Arquitetura peer-to-peer

Pergunta **8**

Respondida

Nota: 10,00 em 10,00

Os dados que circulam nas mensagens de invocação de serviços remotos são convertidos para um formato genérico antes de ser enviados. Indique para cada um dos paradigmas de invocação remota qual a técnica de conversão de dados utilizada.

Remote Method Invocation (RMI) Object Serialization

Remote Procedure Call (SUN [RPC](#)) External Data Representation (XDR)

Web Services Extended Markup Language (XML)

Sockets Network Byte Order

Pergunta **9**

Respondida

Nota: 10,00 em 10,00

Estabeleça a relação entre os componentes do [RPC](#) e a sua funcionalidade:

Pedido: retira os parâmetros da mensagem e coloca-os na pilha para invocar o procedimento do serviço

Resposta: retira o resultados da pilha e passa-os para um formato independente na mensagem

Assegura o encaminhamento das mensagens e o dispatching destas para o stubs

Pedido: retira os parâmetros da pilha passa-os para um formato independente na mensagem

Resposta: passa o resultado da mensagem para a pilha de invocação

Server stub

RPC runtime

Client stub

Pergunta **10**

Respondida

Nota: 10,00 em 10,00

A semântica de uma invocação remota indica a forma como são executados os vários passos que a compõem e quais as possíveis acções e consequências em caso de falha. Estabeleça a relação entre os seguintes tipos de invocação e as suas características.

Se as funções remotas forem idempotentes

Pode-se usar uma semântica At-least-once ou At-most-once

A funcionalidade remota é invocada no máximo uma vez

Semântica tipo At-most-once

A funcionalidade remota pode ou não ser invocada

Semântica tipo Maybe

Se as funções remotas não forem idempotentes

Tem que se utilizar uma semântica At-most-once

A funcionalidade remota é invocada, mas não se sabe exactamente quantas vezes

Semântica tipo At-least-once

Pergunta **11**

Respondida

Nota: 6,00 em 10,00

Estabeleça as correspondências correctas dos componentes do WSDL:

Especifica o endereço do WebService, normalmente um URL

Port

Descreve o formato abstrato da mensagem

Binding

Definição abstracta dos tipos definidos pelo utilizador

Type

Descreve a interface do Web Service

portType

Define o protocolo e com ele o formato das mensagens, de uma forma dependente do protocolo

Message

Pergunta **12**

Respondida

Nota: 10,00 em 10,00

Estabeleça as correspondências correctas das operações do serviço de nomes:

Devolve o identificador associado a um nome

Lookup

Estabelece a associação entre um nome e o identificador de um recurso

Bind

Pergunta **13**

Respondida

Nota: 3,33 em 10,00

Considere a seguinte matriz, onde nas colunas estão representados Objectos, nas linhas estão representados Agentes e cada célula representa os direitos de acesso:

Agentes / Objectos	O1	O2	O3	O4
A1	R	RW	RX	---
A2	RX	---	RW	R

Qual é a Access Control List (ACL) do objeto O2 ?

A1: RW; A2: ---

Esta matriz é usada para que tipo de Controlo de Acesso ?

Uma coluna

As Access Control List (ACL) correspondem a uma coluna ou a uma linha desta matriz ?

Discretionary Access Control (DAC)

Pergunta **14**

Respondida

Nota: 0,00 em 10,00

Considere as 4 mensagens do protocolo Needham - Shroeder entre A, B e a autoridade de certificação S:

1. $A \rightarrow S: A, B, Na$

2. $S \rightarrow A: \{Na, B, Kab, \{Ts, A, Kab\}Kb\}Ka$

3. $A \rightarrow B: \{A, Ta\}Kab, \{Kab, A, Ts\}Kb$

4. $B \rightarrow A: \{Ta + 1\}Kab$

Se A quiser enviar a informação M com privacidade na mensagem 3, deve enviar o seguinte:

3. $A \rightarrow B: \{A, Ta\}Kab, \{Kab, A, Ts, M\}Kb$

Na mensagem 3, o elemento Ts serve para

A saber que a chave de sessão é recente

Quando A recebe a mensagem 4, acredita que ela veio de B porque

Está cifrada com a chave de S

Pergunta **15**

Respondida

Nota: 10,00 em 10,00

Estabeleça a correspondência entre as seguintes afirmações:

Autenticidade	Identificação do agente que produziu a informação
Integridade	A informação está correcta e completa
Não repúdio	Impossibilidade de um agente negar uma acção que efectivamente cometeu
Privacidade	Acesso à informação apenas por agentes autorizados

Pergunta **16**

Respondida

Nota: 10,00 em 10,00

Se A tiver um par (chave pública, chave privada), quais são as afirmações verdadeiras:

Selecione uma ou mais opções de resposta:

- ☒ a. A chave privada de A só pode ser conhecida por A
- ☐ b. A chave privada de A pode ser conhecida por todos os outros agentes
- ☒ c. A chave pública de A pode ser conhecida por todos os outros agentes
- ☐ d. A chave pública de A só pode ser conhecida por A pela autoridade de certificação

Pergunta **17**

Respondida

Nota: 2,00 em 10,00

Estabeleça as relações correctas relativamente à cache do AFS.

O servidor sabe quais os clientes que têm o ficheiro em cache	Ficheiros
O cliente verifica com o servidor se a sua cache ainda está válida	Blocos
Nos clientes a cache é mantida em	Memória
O cliente é avisado quando a sua cache ficar desactualizada	Não
É escalável para centenas ou milhares de clientes	Sim

Pergunta **18**

Respondida

Nota: 2,00 em 10,00

Estabeleça as relações correctas relativamente à cache do NFS.

A cache está organizada por

Ficheiros

O servidor reutiliza a sua cache de blocos de disco

Não reutiliza

O servidor sabe que clientes têm o ficheiro em cache

Sabe

O cliente detecta que a sua cache pode estar desactualizada

Não detecta

Se dois clientes escreverem o mesmo ficheiro simultaneamente, o sistema garante a coerência do ficheiro

Não garante

Pergunta **19**

Respondida

Nota: 7,50 em 10,00

O Coordenador ou um Participante podem falhar durante a execução do protocolo Two-Phase Commit. Isso impacta o funcionamento dos outros nós e quando o nó que falhou recomeçar a funcionar, tem que recuperar o ponto onde estava no protocolo e continuar com o mesmo. Estabeleça as relações entre as afirmações seguintes:

Um participante tem um timeout no estado inicial quando espera a mensagem "Prepare_Commit" do Coordenador

O Participante decide fazer Abort da transacção

O Coordenador obtém um timeout quando espera a resposta à mensagem "Prepare_Commit"

O Coordenador decide fazer Abort da transacção

O Coordenador falha e quando recupera verifica que estava no estado "Confirmar", tinha recebido "Commit" de todos os participantes mas poderia ainda não lhes ter enviado a sua decisão.

O Coordenador reenvia a mensagem "Confirm_Abort" aos participantes

Um Participante falha e quando recupera verifica que estava no estado "Preparado", já depois de ter enviado a sua decisão ao Coordenador

O Participante volta a ficar à espera da mensagem do Coordenador com a decisão sobre a transacção

Pergunta **20**

Respondida

Nota: 10,00 em 10,00

Estabeleça as relações sobre as propriedades das transacções:

Atomicidade Para um observador externo, uma transacção ou se executa na totalidade ou não se executa.

Seriabilidade Se diversas transacções se executarem em paralelo sobre os mesmos objectos, tudo se passa como se as transacções se executassem e

Consistência Cada transacção deve, a partir de um estado inicial válido e caso se execute completamente, atingir um novo estado válido

Persistência Os resultados de uma transacção que confirmou permanecem depois de esta acabar e são supostos sobreviver ao conjunto de faltas exp

Previous Activity

Ir para...

Next Activity