

## 2n Parcial de Teoria (TSR)

Aquest examen consta de 40 qüestions. En cada cas només una de les respostes és correcta. Per a indicar la resposta n'hi ha prou amb emplenar la casella corresponent en la fulla de respostes adjunta. Totes les qüestions tenen el mateix valor. Si són correctes, aporten 0,25 punts a la nota obtinguda. Si són incorrectes descomptaran 1/5 del valor correcte, és a dir, -0,05 punts. Convé pensar acuradament les respostes.

Durada prevista per a aquesta part de l'examen: 2 hores.

### 1. El model de fallades bizantí...

A	...no ha d'assumir-se per a implantar un servei distribuït real ja que els ordinadors no poden tenir aquest comportament.
B	...assumeix que els processos poden tenir un comportament arbitrari.
C	...no té sentit actualment. Com suggereix el seu nom, modela el comportament d'ordinadors obsolets, en lloc d'ordinadors recents.
D	...assumeix que els processos poden fallar parant i que aquestes fallades poden ser detectades per altres processos.
E	Totes les anteriors.
F	Cap de les anteriors.

### 2. Quan dissenyem un algorisme assumint el model de fallades de parada...

A	...l'algorisme resultant serà senzill ja que s'assumeix que els processos es comporten segons la seua especificació fins que fallen.
B	...hi haurà dificultats per a implantar aquest algorisme ja que els sistemes operatius i el middleware no garanteixen un comportament perfecte dels processos.
C	...s'assumeix que els processos fallen parant i que aquestes fallades poden ser detectades pels processos correctes.
D	...s'assumeix que els canals de comunicació funcionen correctament.
E	Totes les anteriors.
F	Cap de les anteriors.

### 3. Hi ha una fallada de partició de la xarxa quan...

A	...un procés para.
B	...un procés mostra un comportament arbitrari.
C	...es fragmenta i distribueix una base de dades entre múltiples ordinadors, però d'una forma incorrecta (p. ex., esborrant algunes files en diverses taules).
D	...el teorema CAP no ha sigut respectat.
E	Totes les anteriors.
F	Cap de les anteriors.

**4. En el model de “partició primària”:**

A	Els subgrups minoritaris (aquells amb menys de la meitat dels nodes) han de parar.
B	Tots els canals de comunicació funcionen correctament.
C	Apliquem el teorema CAP sacrificant la tolerància al particionat.
D	Tots els subgrups de nodes poden continuar.
E	Totes les anteriors.
F	Cap de les anteriors.

**5. La seguretat (*Safety*) és...**

A	...un atribut qualitatiu de la robustesa.
B	...la probabilitat $S(t)$ que un sistema distribuït es recupere en l'instant $t$ si havia fallat en l'instant $t'=0$ .
C	...un model de fallades.
D	...un dels aspectes considerats en el teorema CAP.
E	Totes les anteriors.
F	Cap de les anteriors.

**6. La replicació millora el rendiment d'un servei quan:**

A	...la major part de les operacions són de només lectura.
B	...totes les operacions impliquen escriptures.
C	...les rèpliques estan contínuament recuperant-se de fallades en els seus processos.
D	...s'usa un model de replicació passiva, es perd la connectivitat de la xarxa i les modificacions de l'estat no poden propagar-se a les rèpliques secundàries.
E	Totes les anteriors.
F	Cap de les anteriors.

**7. En el model de replicació passiva:**

A	Múltiples rèpliques reben i processen directament les peticions dels clients.
B	Totes les rèpliques interpreten un mateix paper.
C	Per a implantar-ho no es pot assumir el model de fallades arbitràries.
D	Per a implantar-ho no es pot assumir el model de fallades de parada.
E	Totes les anteriors.
F	Cap de les anteriors.

**8. Sobre els models de consistència centrats en dades:**

A	Causal és més estricte que <i>cache</i> .
B	Processador és més estricte que causal.
C	<i>Cache</i> és més estricte que FIFO.
D	Seqüencial és més estricte que <i>cache</i> .
E	Totes les anteriors.
F	Cap de les anteriors.

**9. L'acoblament mesura:**

A	El grau de dependència entre els mòduls d'una aplicació.
B	La fiabilitat d'una aplicació.
C	La continuïtat de servei.
D	Si cadascuna de les dimensions considerades en el teorema CAP s'està garantint.
E	Totes les anteriors.
F	Cap de les anteriors.

**10. No interessa una cohesió feble perquè:**

A	Sempre genera defectes, errors i fallades.
B	Implica una pèrdua de disponibilitat.
C	La funcionalitat de cada operació no queda clara. Això evita que els mòduls puguin reutilitzar-se en altres aplicacions.
D	Assegura consistència forta entre rèpliques.
E	Totes les anteriors.
F	Cap de les anteriors.

**11. En un sistema distribuït amb acoblament baix:**

A	Els missatges de petició seran xicotets, generalment.
B	Es minimitza la interacció entre components.
C	Hi ha un alt grau de localitat en l'accés a dades.
D	Cada operació solament necessita uns pocs arguments.
E	Totes les anteriors.
F	Cap de les anteriors.

**12. Els magatzems NoSQL...**

A	...asseguren la consistència de dades utilitzant transaccions ACID.
B	...solen ser més escalables que els sistemes gestors de bases de dades relacionals.
C	...no proporcionen persistència de dades.
D	...utilitzen un llenguatge d'interrogació basat en l'operador JOIN.
E	Totes les anteriors.
F	Cap de les anteriors.

**13. Els magatzems clau-valor:**

A	Són exemples de sistemes gestors de bases de dades relacionals.
B	Usen un esquema basat en objectes amb un nombre variable d'atributs.
C	Dos exemples són MongoDB i SimpleDB.
D	Dos exemples són Cassandra i PNUMs.
E	Totes les anteriors.
F	Cap de les anteriors.

**14. Els magatzems de registres extensibles:**

A	Usen esquemes basats en taules amb un nombre variable de columnes.
B	Usen particionat horitzontal i vertical de taules per a millorar l'escalabilitat.
C	Un exemple és Bigtable.
D	Un exemple és Cassandra.
E	Totes les anteriors.
F	Cap de les anteriors.

**15. Sobre el teorema CAP:**

A	Relaciona consistència, disponibilitat i tolerància al particionat.
B	El seu resultat solament té sentit en sistemes distribuïts sincrònics.
C	Estableix que la consistència forta i l'alta disponibilitat no poden proporcionar-se simultàniament.
D	Relaciona consistència de dades, atomaticitat i persistència.
E	Totes les anteriors.
F	Cap de les anteriors.

**16. Sobre les conseqüències del teorema CAP:**

A	Per a implantar un servei altament disponible i tolerant a particions, necessitem utilitzar consistència eventual (o final).
B	Per a implantar un servei amb consistència forta (seqüencial) i altament disponible, no podem permetre particions de la xarxa.
C	La consistència eventual és pràcticament obligatòria per a implantar serveis escalables ja que aquests han de ser altament disponibles i tolerar particions.
D	El model de “partició primària” s'assumeix per a sacrificar la disponibilitat, gestionar particions i assegurar consistència forta.
E	Totes les anteriors.
F	Cap de les anteriors.

**17. Les tres dimensions de l'escalabilitat són:**

A	Consistència, disponibilitat i tolerància a particions.
B	Fiabilitat i els dos tipus de seguretat ( <i>security</i> i <i>safety</i> ).
C	Hardware, firmware i programari.
D	Interfície d'usuari, lògica de negoci i dades persistents.
E	Totes les anteriors.
F	Cap de les anteriors.

**18. L'escalabilitat vertical consisteix en:**

A	Adaptar la capacitat de còmput a la càrrega actual.
B	Assegurar continuïtat de servei durant les actualitzacions de programari.
C	Incrementar el nombre de nodes en els quals un servei està executant-se.
D	Incrementar la capacitat de còmput d'un node determinat.
E	Totes les anteriors.
F	Cap de les anteriors.

**19. L'escalabilitat horitzontal consisteix en:**

A	Adaptar la capacitat de còmput a la càrrega actual.
B	Assegurar continuïtat de servei durant les actualitzacions de programari.
C	Incrementar el nombre de nodes en els quals un servei està executant-se.
D	Incrementar la capacitat de còmput d'un node determinat.
E	Totes les anteriors.
F	Cap de les anteriors.

**20. Els quatre mecanismes complementaris per a aconseguir escalabilitat de grandària són:**

A	Fiabilitat, disponibilitat, mantenibilitat i seguretat.
B	Repartiment de tasques, repartiment de dades, replicació i ús de memòries cau.
C	Consistència estricta, particionat de taules, replicació activa i tolerància a particions.
D	Elasticitat, computació en el núvol, computació grid i computació P2P.
E	Totes les anteriors.
F	Cap de les anteriors.

**21. Propietats dels algorismes descentralitzats:**

A	Quan un procés falla, l'algorisme es bloqueja.
B	Els processos prenen decisions utilitzant informació local.
C	Els processos assumeixen que existeix un rellotge global.
D	Un dels processos té informació completa sobre l'estat del sistema.
E	Totes les anteriors.
F	Cap de les anteriors.

**22. El particionat horitzontal de taules millora l'escalabilitat perquè...**

A	És un mecanisme de repartiment de dades.
B	Proporciona equilibrat de càrrega.
C	Incrementa el grau de concurrència, així el servei resultant pot processar un major nombre de peticions simultàniament.
D	Amb un disseny apropiat, no necessita cap pas de sincronització.
E	Totes les anteriors.
F	Cap de les anteriors.

**23. Un servei és elàstic quan...**

A	És fiable i altament disponible.
B	És robust i utilitza un model de consistència ràpid.
C	És escalable i s'adapta dinàmica i autònomament.
D	És segur i tolerant a defectes ( <i>fault-tolerant</i> ).
E	Totes les anteriors.
F	Cap de les anteriors.

**24. Per a implantar un servei elàstic, necessitem:**

A	Un sistema de monitoratge de la càrrega actual.
B	Un sistema reactiu que automatitzi la reconfiguració del servei, prenent decisions d'escalat.
C	Un sistema reactiu que tinga en compte el SLA.
D	Un sistema de monitoratge del rendiment actual.
E	Totes les anteriors.
F	Cap de les anteriors.



**25. Els objectius principals de la seguretat (*security*) són:**

A	Assegurar la persistència i consistència de les dades.
B	Confidencialitat, integritat, disponibilitat i comptabilitat.
C	Seguretat ( <i>safety</i> ), fiabilitat, disponibilitat i mantenibilitat.
D	Transparència, continuïtat de servei, rendiment i eficiència.
E	Totes les anteriors.
F	Cap de les anteriors.

**26. L'objectiu d'una política de seguretat és:**

A	Assegurar la correcció d'un sistema de seguretat.
B	Implantar un sistema de seguretat.
C	Especificar un sistema de seguretat.
D	Avaluar la robustesa d'un sistema.
E	Totes les anteriors.
F	Cap de les anteriors.

**27. Sobre els mecanismes de seguretat:**

A	Són tècniques i eines utilitzades per a implantar la seguretat.
B	Hi ha tres classes principals: físics, relacionats amb autenticació i relacionats amb autorització (és a dir, control d'accés).
C	Un exemple és l'ús de contrasenyes.
D	Un exemple és la paraula de protecció en els sistemes de fitxers UNIX.
E	Totes les anteriors.
F	Cap de les anteriors.

**28. Una amenaça és:**

A	Una feblesa en dispositius, protocols, programes o polítiques d'un sistema.
B	La probabilitat $A(t)$ que un sistema realitzi les seues funcions en l'instant $t$ si ha estat funcionant correctament des de l'instant $t'=0$ .
C	Un model que especifica quines divergències estan permeses en les rèpliques d'una determinada dada.
D	Un conjunt de regles que especifica quines accions estan autoritzades per als agents d'un sistema determinat.
E	Totes les anteriors.
F	Cap de les anteriors.

**29. Exemples de vulnerabilitats en les polítiques de seguretat:**

A	Denegació de servei.
B	<i>Man in the middle.</i>
C	<i>SYN floods.</i>
D	Falta de plans per a recuperació de desastres.
E	Totes les anteriors.
F	Cap de les anteriors.

**30. Exemples de vulnerabilitats de configuració:**

A	Amenaces desestructurades.
B	Permetre contrasenyes febles.
C	Rastrejadors de paquets.
D	<i>Phishing.</i>
E	Totes les anteriors.
F	Cap de les anteriors.

**31. Sobre els mecanismes en els protocols criptogràfics:**

A	Un MAC assegura no repudi.
B	Un certificat és un mecanisme que proporciona comptabilització.
C	Les funcions unidireccionals (cripto-hashing) s'utilitzen en els MAC i en els certificats.
D	El xifrat simètric necessita dues claus diferents i complementàries, una per a xifrar i una altra per a desxifrar.
E	Totes les anteriors.
F	Cap de les anteriors.

**32. Protocols criptogràfics. Distribució de claus:**

A	Amb xifrat simètric, només necessitem distribuir la clau privada.
B	Amb xifrat asimètric, només necessitem distribuir la clau pública.
C	En el xifrat simètric, la fugida d'informació no és problemàtica.
D	En el xifrat asimètric, necessitem canals secrets per a distribuir claus.
E	Totes les anteriors.
F	Cap de les anteriors.

**33. En el patró bàsic (i sincrònic) de petició/resposta:**

A	Les peticions dels clients poden lliurar-se en un ordre "no FIFO" al servidor.
B	El client pot enviar una altra petició abans de rebre la resposta per a l'actual.
C	Si el servidor cau abans de respondre una petició d'un client, aquest client quedarà bloquejat.
D	Aquest patró s'implanta utilitzant sockets PUSH i PULL en ZeroMQ.
E	Totes les anteriors.
F	Cap de les anteriors.

**34. Per a desplegar el patró bàsic petició/resposta, considerant sockets ZeroMQ:**

A	Els clients realitzen el bind() i els servidors el connect().
---	---

B	Els servidors realitzen el bind() i els clients el connect().
C	Tant els clients com els servidors usen un únic socket. Tots dos realitzen un bind(), però també un connect() sobre altres sockets.
D	No es necessita cap socket per a implantar aquest patró arquitectònic.
E	Totes les anteriors.
F	Cap de les anteriors.

**35. El patró arquitectònic PUSH-PULL bàsic és un patró de comunicacions...**

A	Bidireccional.
B	Sincrònic.
C	Per a fer multienviaments ( <i>multicast</i> ).
D	Asincrònic.
E	Totes les anteriors.
F	Cap de les anteriors.

**36. En el patró arquitectònic client/servidor avançat amb múltiples clients i múltiples servidors interconnectats mitjançant una cua intermèdia:**

A	Cada servidor és un únic punt de fallada per al servei.
B	La cua intermèdia és un element estable. En la seua configuració més simple, els seus sockets faran el bind().
C	La cua intermèdia utilitza sockets PUSH-PULL.
D	Els clients utilitzen sockets SUB.
E	Totes les anteriors.
F	Cap de les anteriors.

**37. Els *heart-beats* s'utilitzen en algunes arquitectures client-servidor per a:**

A	Detectar fallades en els clients.
B	Monitoritzar la càrrega actual.
C	Millorar l'escalabilitat dels servidors.
D	Implantar protocols criptogràfics.
E	Totes les anteriors.
F	Cap de les anteriors.

**38. Els reintents s'utilitzen en algunes arquitectures client-servidor avançades per a:**

A	Detectar fallades en els servidors.
B	Implantar un mecanisme d'equilibrat de càrrega.
C	Millorar l'escalabilitat dels servidors.
D	Detectar fallades en els clients, combinant-los amb <i>timeouts</i> .
E	Totes les anteriors.
F	Cap de les anteriors.

**39. Per a implantar un mecanisme de recuperació en cas de fallada d'una petició no idempotent, necessitem:**

A	Identificar clarament cada missatge de petició, amb un parell <id-emissor, id-petició>.
B	Abans de servir cada petició, el servidor ha de cercar-la en el seu "magatzem de respostes".
C	Si trobem una petició en el "magatzem de respostes", la resposta és presa d'allí i enviada al client.
D	Després de servir cada petició, el servidor copia el seu missatge de resposta en el "magatzem de respostes" local.
E	Totes les anteriors.
F	Cap de les anteriors.

**40. En els patrons arquitectònics client/servidor avançats del tema 9, els servidors es repliquen de la següent manera:**

A	Utilitzant el model de replicació actiu.
B	Exigint que totes les seues operacions siguen idempotents.
C	Utilitzant el model de replicació passiu.
D	Tant el procés primari com els secundaris utilitzen un mòdul de “ <i>heart-beats</i> ” per a detectar fallades en els clients.
E	Totes les anteriors.
F	Cap de les anteriors.