

Commencé le	mercredi 18 décembre 2019, 13:30
État	Terminé
Terminé le	mercredi 18 décembre 2019, 16:00
Temps mis	2 heures 30 min
Points	57,00/80,00
Note	14,25 sur 20,00 (71%)

Question 1
Partiellement correct
Note de 3,00 sur 8,00

Pour chacune des déclarations suivantes, indiquez si elles sont vraies ou fausses.

Attention: si une réponse correcte apporte des points (1/(total de la question)), une réponse incorrecte en retire la même quantité. Ne pas répondre n'ajoute pas ni ne retire de points. La note finale de la question ne pourra pas descendre en dessous de zéro, et ne pourra donc pas avoir une note négative sur le total de l'examen.

For each of the following statements, indicate whether they are true or false.

Warning: if a correct answer adds points (1/(total of the question)), an incorrect answer removes the same amount. If you chose not to answer for a statement, it does not add nor remove points. The final grade of the question can not go below zero, and therefore can not have a negative note on the total of the exam.

DNS est généralement délégué hiérarchiquement en ayant, par exemple, les nœuds racine indiquant aux résolveurs quels serveurs interroger pour ".ca", et ainsi de suite, jusqu'à ce que la requête du client puisse être répondue.

Vrai / True



DNS is delegated hierarchically by having, e.g., the root nodes tell resolvers which servers to query for ".ca", and so on, until the client's query can be answered.

Les résolveurs DNS (Domain Name System) utilisent Paxos et des messages d'invalidation pour maintenir la cohérence des enregistrements mis en cache.

Faux / False



Domain Name System (DNS) resolvers use Paxos and invalidation messages to maintain the consistency of cached records.

Si le serveur avec lequel un client communique ne prend en charge aucune forme de chiffrement (par exemple, https), le client doit utiliser un VPN afin que personne ne puisse écouter son trafic.

Vrai / True



If the server a client communicates with does not support any form of encryption (e.g., https), the client should use a VPN so that nobody can overhear its traffic.

Certains réseaux de distribution de contenu (CDN) utilisent des réponses DNS pour diriger les clients vers le cache CDN le plus proche.



Some Content Delivery Networks (CDNs) use DNS responses to direct clients to the closest CDN cache.

Le but de la paravirtualisation (par exemple, Xen) est de faire complètement ignorer au système d'exploitation invité qu'il s'exécute sur une machine virtuelle.

Faux / False



The goal of paravirtualization (e.g., Xen) is to make the guest operating system completely unaware that it is running on a virtual machine.

L'exclusion mutuelle distribuée en anneau est une excellente solution pour une application sensible à la latence exécutée sur 10 000 nœuds.

Faux / False



Ring-based distributed mutual exclusion is a great solution for a latency-sensitive application running on 10,000 nodes.

Un système de fichiers NFS apparaît sur le même chemin de fichier sur tous les clients.

Faux / False



An NFS file system appears at the same file path on all clients.

Un système de fichiers AFS apparaît sur le même chemin de fichier sur tous les clients.

Faux / False



An AFS file system appears at the same file path on all clients.

Réponses:

- Vrai
- Faux
- Faux
- Vrai
- Faux
- Faux
- Faux
- Vrai

Question 2

Incorrect

Note de 0,00 sur 2,00

Parmi les éléments suivants, sélectionnez celui ou ceux qui sont vrai(s). / Among the following statements, select the one(s) that are true.

Veuillez choisir au moins une réponse :

- ☐ a. Le bind mount est l'option préférée aux volumes pour partager des fichiers de configuration depuis l'hôte vers les containers. / Bind mount is better than volumes to share configuration files from the host machine to containers.
- ☒ b. Un volume docker permet d'échanger des données entre les containers, et est effacé à la suppression du container. / A docker volume provide a way to share data between containers, and is deleted at the same time when the container is deleted ✗
- ☐ c. La commande `docker run -p 127.0.0.1:80:8080/tcp ubuntu bash` expose le port 80 du container sur le port 8080 de l'hôte / The command `docker run -p 127.0.0.1:80:8080/tcp ubuntu bash` binds port 80 of the container to TCP port 8080 on host
- ☒ d. Vous venez de mettre en place un serveur de stockage réparti, il est possible de le monter sur l'hôte et d'y accéder dans le container via un bind mount. / You just setup a shared storage server, and it is possible to access it, after mounting it on the host, in the container thanks to the bind mount. ✓

Votre réponse est incorrecte.

Les réponses correctes sont : Vous venez de mettre en place un serveur de stockage réparti, il est possible de le monter sur l'hôte et d'y accéder dans le container via un bind mount. / You just setup a shared storage server, and it is possible to access it, after mounting it on the host, in the container thanks to the bind mount. , Le bind mount est l'option préférée aux volumes pour partager des fichiers de configuration depuis l'hôte vers les containers. / Bind mount is better than volumes to share configuration files from the host machine to containers.

Question 3

Partiellement correct

Note de 1,00 sur 2,00

Parmi les éléments suivants à propos du stockage réparti, sélectionnez celui ou ceux qui sont vrai(s).

Among the following statements about distributed storage, select the one(s) that are true.

Veillez choisir au moins une réponse :

- ☐ a. Un volume est un partage hébergé par les serveurs et peut être construit par un ensemble de sous-volumes, généralement hébergés par différents serveurs. / A volume is a share hosted by servers and can be composed by a set of subvolumes, usually hosted by different servers
- ☐ b. Le mode distribué permet que chaque élément écrit sur une « *brick* » soit répliqué N fois sur d'autres « *bricks* » sur des noeuds du cluster. / Distributed mode allows each element written on a brick to be replicated N times on other bricks on nodes in the cluster
- ☒ c. Il est possible de monter un dossier glusterFS partagé via la commande mount à l'aide de FUSE / It is possible to mount a glusterFS shared folder via the mount command using FUSE ✓
- ☐ d. GlusterFS utilise un serveur de metadata pour structurer les fichiers / GlusterFS uses a metadata server to structure files

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 1.

Les réponses correctes sont : Il est possible de monter un dossier glusterFS partagé via la commande mount à l'aide de FUSE / It is possible to mount a glusterFS shared folder via the mount command using FUSE, Un volume est un partage hébergé par les serveurs et peut être construit par un ensemble de sous-volumes, généralement hébergés par différents serveurs. / A volume is a share hosted by servers and can be composed by a set of subvolumes, usually hosted by different servers

Question 4

Incorrect

Note de 0,00 sur 2,00

Avec laquelle des commandes suivantes puis-je connaître les enregistrements **MX** du nom de domaine **polymtl.ca** ? Cocher l'affirmation vraie.

Which of the following commands can I use to know the **MX** records of the domain name **polymtl.ca** ? Check the only true statement.

Veillez choisir une réponse :

- ☐ a.
- ☐ b.
- ☐ c.
- ☒ d.

✗

Votre réponse est incorrecte.

La réponse correcte est :

Question 5

Incorrect

Note de 0,00
sur 2,00

Parmi les éléments suivants à propos des transactions, sélectionnez celui ou ceux qui sont vrai(s).

Among the following statements about transactions, select the one(s) that are true.

Veuillez choisir au moins une réponse :

- ☒ a. Avec le niveau d'isolation **READ UNCOMMITTED**, une requête **SELECT** verra toujours les derniers changements commis, même s'ils ont été faits dans une autre session, après le début de la transaction / With the isolation level **READ UNCOMMITTED**, a **SELECT** request will always see the last committed changes, even if they were made in another session, after the transaction starts ✖
- ☐ b. Les requêtes de modification et de suppression posent un verrou partagé sur les lignes concernées par la clause WHERE d'une requête, tandis que les requêtes d'insertion posent un verrou exclusif / Modification and suppression requests place a shared lock on the lines affected by the WHERE clause of a request, while insertion requests place an exclusive lock
- ☒ c. Un verrou partagé sur les lignes x va permettre aux autres sessions d'obtenir également un verrou partagé sur les lignes x, mais pas d'obtenir un verrou exclusif / A shared lock on x lines will allow other sessions to also get a shared lock on x lines, but not get an exclusive lock ✔
- ☐ d. Dans une base de données, les verrous de ligne s'utilisent avec les transactions, et dépendent des index / In a database, line locks are used with transactions, and depend on indexes

Votre réponse est incorrecte.

Les réponses correctes sont : Dans une base de données, les verrous de ligne s'utilisent avec les transactions, et dépendent des index / In a database, line locks are used with transactions, and depend on indexes, Un verrou partagé sur les lignes x va permettre aux autres sessions d'obtenir également un verrou partagé sur les lignes x, mais pas d'obtenir un verrou exclusif / A shared lock on x lines will allow other sessions to also get a shared lock on x lines, but not get an exclusive lock

Question 6

Incorrect

Note de 0,00
sur 2,00

Kubernetes est un système d'orchestration de containers d'applications sur des grappes de serveurs composées: (sélectionnez la ou les réponses applicable(s))

Kubernetes is a system of orchestration of application containers on clusters of servers composed: (select the applicable answer (s))

Veuillez choisir au moins une réponse :

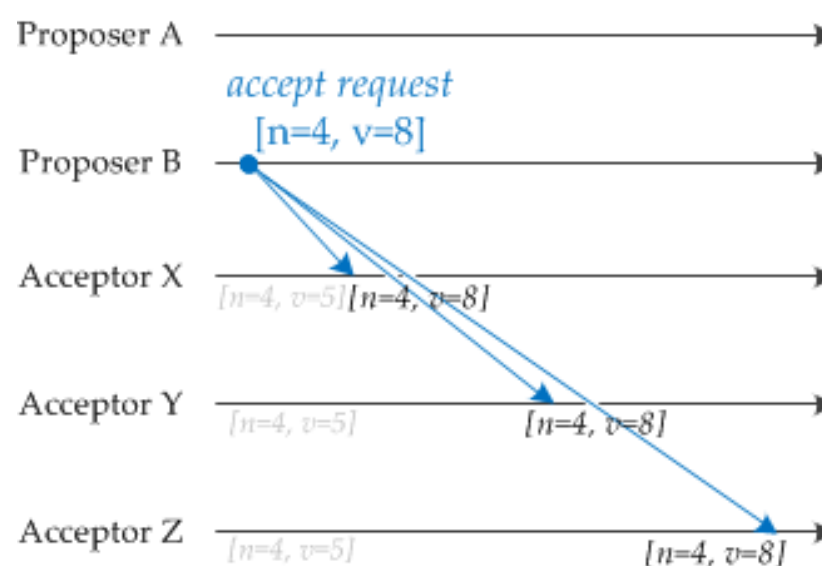
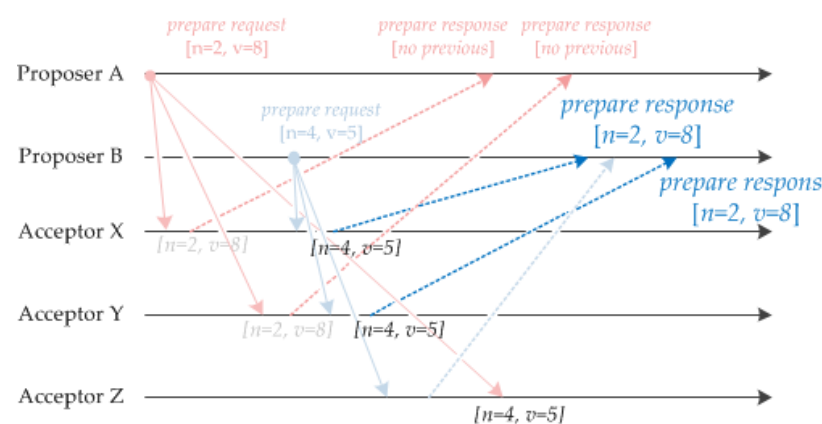
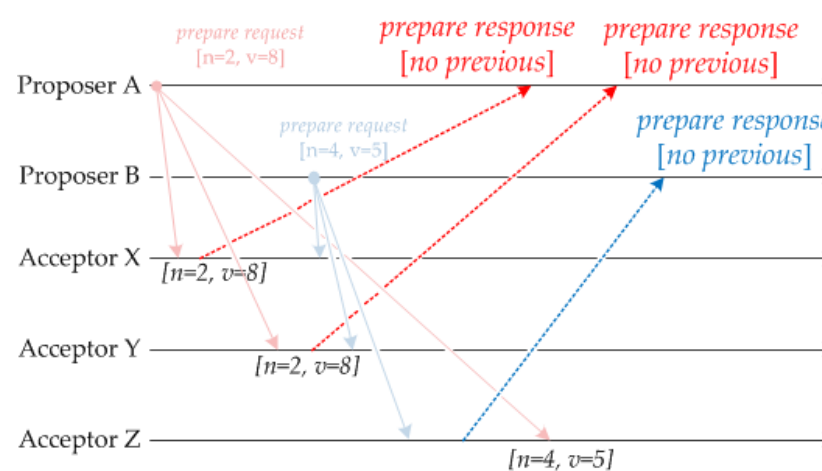
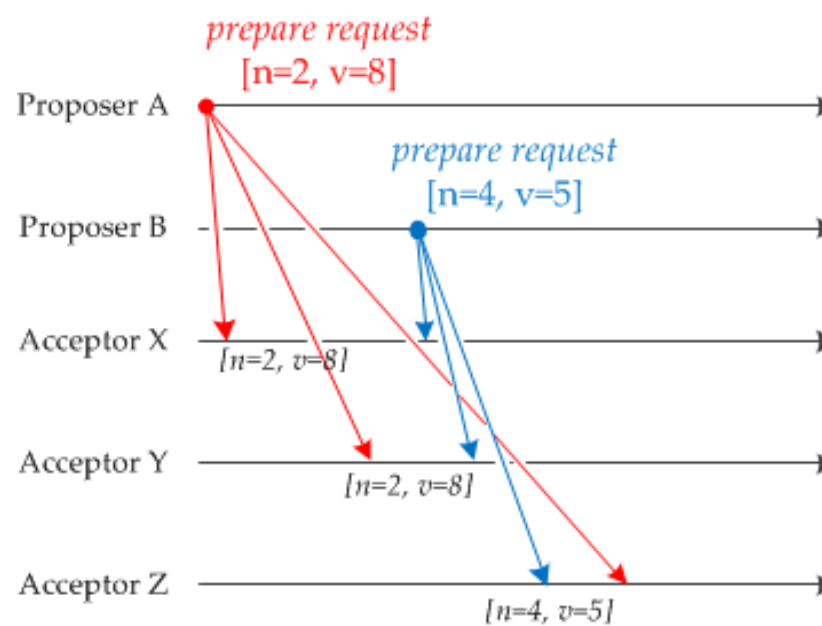
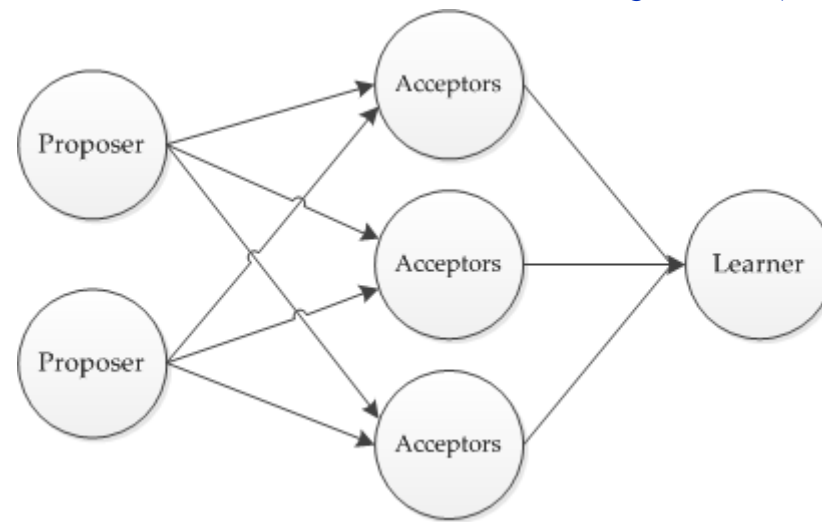
- ☐ a. de « pods » qui sont des machines qui coordonnent la planification et la gestion des conteneurs d'applications sur le cluster / of "pods" which are machines that coordinate the planning and management of application containers on the cluster
- ☐ b. de « nodes » qui sont des groupes d'un ou plusieurs containers d'applications et qui partagent des volumes partagés et une même adresse IP / of "nodes" which are groups of one or more application containers and share shared volumes and the same IP address
- ☒ c. de « nodes », groupe de pods travaillant ensemble / of "nodes", group of pods working together ✖
- ☒ d. de « pods » qui sont des groupes d'un ou plusieurs containers d'applications et qui partagent des volumes partagés et une même adresse IP / of "pods" which are groups of one or more application containers and share shared volumes and the same IP address ✔
- ☐ e. de « nodes » où sont déployés les applications / of "nodes" where the applications are deployed

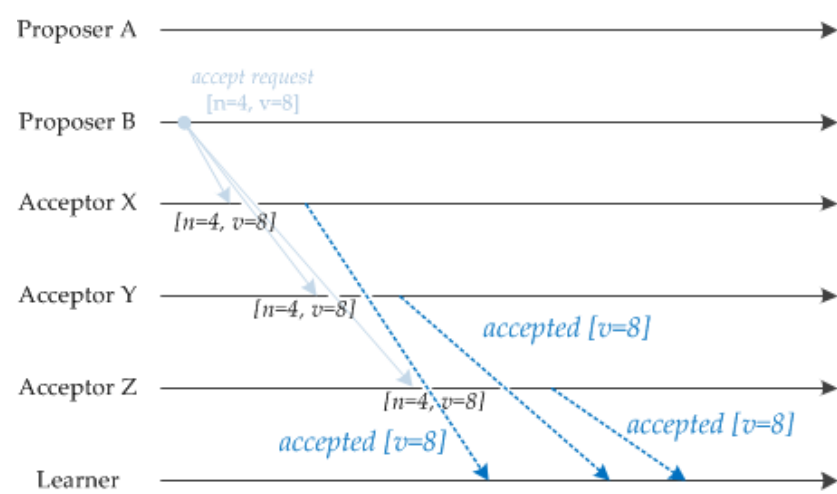
Votre réponse est incorrecte.

Les réponses correctes sont : de « nodes » où sont déployés les applications / of "nodes" where the applications are deployed, de « pods » qui sont des groupes d'un ou plusieurs containers d'applications et qui partagent des volumes partagés et une même adresse IP / of "pods" which are groups of one or more application containers and share shared volumes and the same IP address

Les figures suivantes ont été vues en cours et proviennent de [Paxos By Example](#) (lien pour référence, non disponible durant l'examen).

The following figures were seen during the lectures and come from [Paxos By Example](#) (link for reference, not available during the exam).





Question 7

Terminer

Note de 3,00
sur 3,00

Considérez une implémentation de l'algorithme Paxos où un proposeur attend que moins d'une majorité d'accepteurs répondent OK à un message Préparer ou Accepter avant de passer à l'exécution des étapes suivantes. Expliquez comment une telle implémentation peut briser les garanties Paxos.

Consider an implementation of the Paxos algorithm where a proposer waits for less than a majority of acceptors to answer OK to a Prepare or an Accept message before it proceeds to executing the next steps. Explain how such an implementation can break the Paxos guarantees.

Parmi les garanties offertes par Paxos, nous avons la robustesse et la garantie de toujours arriver à un consensus. Ainsi, Paxos nous garanti d'avoir un seul bon résultat considéré par tous (par exemple un seul serveur maître). Ce qui arriverait si un proposeur attend moins d'une majorité d'Accepteurs qui répondent OK, est qu'on pourrait se retrouver avec plusieurs proposeurs qui seraient considérés comme serveur maître brisant la garantie de consensus de Paxos (Ce problème pourrait être obtenu dans un réseau partitionné).

Une majorité d'accepteurs peut déjà avoir choisi une valeur différente. Le proposeur peut obtenir des réponses d'accepteurs extérieurs à cette majorité et peut procéder à la proposition, puis valider une nouvelle valeur (ce qui casse la propriété selon laquelle une seule valeur peut être choisie à la suite de l'exécution d'une instance Paxos).

Commentaire :

Question 8

Terminer

Note de 3,00
sur 3,00

Expliquez pourquoi Paxos ne peut pas tolérer n fautes avec moins de $2n + 1$ nœuds.

Explain why Paxos cannot tolerate n failures with less than $2n + 1$ nodes.

Paxos requiert toujours une majorité de votes, soient plus que la moitié du nombre de nœuds présents (avec $2n+1$ la majorité est $n+1$). Avec $2n + 1$ nœuds, si nous avons n fautes, la majorité peut toujours être obtenue car il reste toujours $n+1$ nœuds fonctionnels. Cependant, avec moins de $2n+1$ nœuds on n'aura pas cette majorité, ce qui explique qu'on ne peut pas tolérer n fautes (par exemple avec $2n$ nœuds il restera n nœuds donc moins que la majorité).

Supposons que nous essayons de tolérer n fautes avec seulement $2n$ nœuds. Si n nœuds faillissent, un proposeur ne peut pas entendre la majorité des accepteurs ($n+1$ nœuds), et une valeur ne sera jamais choisie.

Commentaire :

Question 9

Terminer

Note de 5,00
sur 6,00

Une hypothèse courante dans Paxos est que différents
proposeurs utilisent des numéros de proposition différents.
Un collègue vous montre une implémentation de Paxos où:

1. Différents proposeurs peuvent utiliser les mêmes numéros de proposition, et
2. Un accepteur rejette un message « *Prepare* » ou « *Accept* » uniquement si le numéro de proposition dans le message est strictement inférieur au plus grand numéro de proposition que l'accepteur a vu (c'est-à-dire exactement comme présenté en classe et dans les notes de cours).

One common assumption in Paxos is that different
proposers use different proposal numbers. A colleague
shows you an implementation of Paxos where:

1. Different proposers can use the same proposal numbers, and
2. An acceptor rejects a "Prepare" or "Accept" message only if the proposal number in the message is strictly smaller than the largest proposal number that acceptor has seen (i.e., exactly as presented in class and in the course notes).

Cette implémentation de Paxos est-elle correcte? Trouvez
un contre-exemple ou expliquez brièvement pourquoi elle
est correcte.

Is this Paxos implementation correct? Find a
counterexample or explain briefly why it is correct.

Non cette implémentation n'est pas correcte. En effet, ce qui se passerait ici est qu'on pourrait avoir 2 proposeurs qui envoient des messages avec le même numéros de séquence. Les 2 auraient une promesse de l'accepteur et les 2 enverraient des messages accept qui seraient validés. On aurait donc pas la garantie du même résultat dépendamment de l'ordre dans lequel les demandes d'acceptation sont reçues. Contre exemple: avec 2 proposeurs (A et B) et 3 accepteurs comme la figure plus haut, si A et B avaient tous 2 $n = 2$, les 2 finiront par envoyer des demandes d'acceptation avec 5 et 8 comme valeur et dépendamment de l'ordre on aurait différent serveur maître.

Si on considère que le problème décrit plus haut n'en est pas un, l'implémentation serait correcte vu qu'on arrive à un consensus malgré tout.

Cette implémentation n'est pas correcte.

Contre-exemple: considérons trois nœuds A, B et C. En même temps, A et B veulent être des proposeurs et proposer différentes valeurs V_A et V_B , avec le même numéro de proposition. En raison des messages perdus, ils n'atteignent que C (A ne reçoit pas le message de B, et B ne reçoit pas le message de A). C validera leurs deux propositions, et acceptera donc à la fois V_A et V_B . A et B penseront avoir une majorité (A + C pour A, ce qui fait 2/3, et B + C pour B, ce qui fait aussi 2/3) et on aura donc deux valeurs possibles en fin de processus, ce qui ne respecte pas les garanties Paxos.

Commentaire :

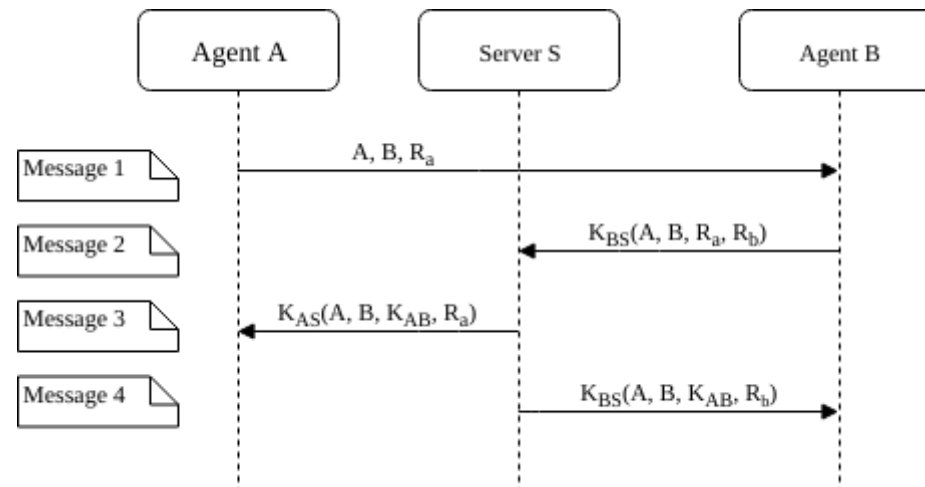
Question 10

Incorrect

Note de 0,00 sur 6,00

La figure suivante illustre un protocole entre deux agents A et B et un serveur S. L'objectif est d'obtenir que le serveur génère une clé de session partagée K_{AB} et de permettre à A et B de s'assurer qu'ils communiquent entre eux.

Chaque agent partage une clé privée avec le serveur S: A a K_{AS} et B a K_{BS} . Les valeurs R_a et R_b sont des « nonces » (nombre utilisé une fois) générés aléatoirement. La notation $K(M_1, M_2, \dots, M_n)$ signifie générer un message contenant une version chiffrée de la séquence M_1, M_2, \dots, M_n à l'aide de la clé K .



Supposons ce qui suit:

- Initialement, seuls A et S connaissent K_{AS} et seuls B et S connaissent K_{BS} .
- Le vrai serveur S n'est pas malveillant, mais il pourrait y avoir un imposteur S_{imp} essayant de se faire passer pour S.
- Il pourrait y avoir un imposteur A_{imp} ou B_{imp} essayant de se faire passer pour A ou B.
- Les imposteurs peuvent intercepter tout trafic, rejouer d'anciens messages ou en injecter de nouveaux.
- Le chiffrement est sécurisé et la forme chiffrée de la séquence ne révèle aucune information sur la forme chiffrée des éléments individuels. Par exemple, connaître $K(M_1, M_2)$ ne révèle aucune information sur $K(M_1)$ ou $K(M_2)$.
- Nous dirons qu'un message est fraîchement généré s'il doit avoir été créé quelque temps après le message initial dans le protocole (c'est à dire que ce n'est pas un message répété, probablement par un imposteur).

Parmi les éléments suivants à propos de ce protocole, sélectionnez celui ou ceux qui sont vrai.

The following figure illustrates a protocol between two agents A and B, and a server S. The intent is to get the server to generate a shared session key K_{AB} , and to also enable A and B to make sure they are communicating with each other.

Each agent shares a private key with the server S: A has K_{AS} , and B has K_{BS} . Values R_a and R_b are randomly generated "nonces" (number-used-once). The notation $K(M_1, M_2, \dots, M_n)$ means to generate a message containing an encrypted version of the sequence M_1, M_2, \dots, M_n using key K .

Assume the following:

- Initially, only A and S know K_{AS} , and only B and S know K_{BS} .
- The true server S is not malicious, but there could be an imposter S_{imp} trying to pose as S.
- There could be an imposter A_{imp} or B_{imp} trying to pose as A or B.
- Imposters can intercept any traffic, replay old messages, or inject new ones.
- The encryption is secure, and the encrypted form of the sequence does not reveal any information about the encrypted form of the individual elements. For example, knowing $K(M_1, M_2)$ does not reveal any information about $K(M_1)$ or $K(M_2)$.
- We will say that a message is freshly generated if it must have been created some time after the initial message in the protocol (i.e. it is not a repeated message, probably by an imposter).

Among the following statements about this protocol, select the one(s) that are true.

Veuillez choisir au moins une réponse :

- ☐ a. À la fin du protocole, B peut être certain d'avoir établi une session avec A. / Upon completion of the protocol, B can be certain that it has established a session with A.
- ☒ b. A peut être certain que le message 3 a été fraîchement généré par S. / A can be certain that message 3 was freshly generated by S. ✓ Seul quelqu'un qui connaissait K_{AS} aurait pu générer $K_{AS}(R_a)$
- ☐ c. Une fois le protocole terminé, personne d'autre que A, B ou S ne peut connaître la valeur de K_{AB} . / Upon completion of the protocol, no one other than A, B, or S can know the value of K_{AB} .
- ☐ d. B peut être certain que le message 4 a été fraîchement généré par S. / B can be certain that message 4 was freshly generated by S.
- ☒ e. S peut être certain que le message 2 a été fraîchement généré par B. / S can be certain that message 2 was freshly generated by B. ✗ Cela pourrait être une répétition d'un ancien message, car il n'y a pas de garantie que R_a est fraîchement généré.
- ☐ f. À la fin du protocole, A peut être certain d'avoir établi une session avec B. / Upon completion of the protocol, A can be certain that it has established a session with B.

Votre réponse est incorrecte.

Les réponses correctes sont : A peut être certain que le message 3 a été fraîchement généré par S. / **A can be certain that message 3 was freshly generated by S.**, B peut être certain que le message 4 a été fraîchement généré par S. / **B can be certain that message 4 was freshly generated by S.**, À la fin du protocole, A peut être certain d'avoir établi une session avec B. / **Upon completion of the protocol, A can be certain that it has established a session with B.**, Une fois le protocole terminé, personne d'autre que A, B ou S ne peut connaître la valeur de K_{AB} . / **Upon completion of the protocol, no one other than A, B, or S can know the value of K_{AB} .**

Question 11

Correct

Note de 4,00 sur 4,00

Soient les variables i, j, k, m et n sauvegardées dans une base de données pour laquelle un système de transactions est en place. Le système tombe en panne, et lors du démarrage du système de remplacement, celui-ci récupère dans la base de données les valeurs actuellement enregistrées des variables, qui sont les suivantes:

- $i = 10$
- $j = 20$
- $k = 30$
- $m = 40$
- $n = 50$

Le système possède aussi un fichier journal pour les opérations qui n'ont pas encore eu le temps d'être sauvegardées sur disque. Lors du démarrage du système de remplacement, le journal est le suivant:

- P0: ...;
- P1: Écrire($m, 12$);
- P2: Écrire($j, 11$);
- P3: Écrire($n, 9$);
- P4: Prépare U($m:P1, j:P2$), P0;
- P5: Compléter U, P4;
- P6: Prépare W($n:P3$), P0;
- P7: Compléter W, P6;
- P8: Écrire($j, 34$);
- P9: Préparer T($j:P8$), P7;
- P10: Compléter T, P9;
- P11: Écrire($k, 42$);
- P12: Prépare V($k:P11$), P10;
- P13: Compléter V, P12;

À l'aide de ces informations, et en considérant qu'aucune nouvelle opération n'est acceptée durant la récupération, indiquez les valeurs des variables une fois que le nouveau système est revenu dans un état cohérent.

- $i =$ ✓
- $j =$ ✓
- $k =$ ✓
- $m =$ ✓
- $n =$ ✓

Let the variables i, j, k, m and n be saved in a database for which a transaction system is in place. The system breaks down, and when the replacement system starts, it recovers from the database the currently recorded values of the variables, which are as follows:

- $i = 10$
- $j = 20$
- $k = 30$
- $m = 40$
- $n = 50$

The system also has a log file for operations that have not yet had the time to be saved to disk. When starting the replacement system, the log is as follows:

- P0: ...;
- P1: Write($m, 12$);
- P2: Write($j, 11$);
- P3: Write($n, 9$);
- P4: Prepare U($m:P1, j:P2$), P0;
- P5: Complete U, P4;
- P6: Prepare W($n:P3$), P0;
- P7: Complete W, P6;
- P8: Write($j, 34$);
- P9: Prepare T($j:P8$), P7;
- P10: Complete T, P9;
- P11: Write ($k, 42$);
- P12: Prepare V($k:P11$), P10;
- P13: Complete V, P12;

Using this information, and considering that no new operations are accepted during recovery, indicate the values of the variables once the new system has returned to a consistent state.

On lit le journal à l'envers et on regarde les dernières transactions complétées pour chaque variable, on voit alors que:

- P13 complète V, qui définit $k=42$
- P10 complète T, qui définit $j=34$
- P7 complète W, qui définit $n=9$
- P5 complète U, qui définit $m=12$ et $j=11$, mais j est ignorée car elle est redéfinie plus récemment par T (en P10)

La seule variable qui n'est pas dans le journal est i , ce qui veut donc dire qu'elle conserve sa valeur telle qu'actuellement dans la base de données, qui est de 10. On a donc:

- $i = 10$
- $j = 34$
- $k = 42$
- $m = 12$
- $n = 9$

Description

Pour les questions suivantes, les transactions T, U & V et l'ordre relatif de leurs opérations sont les mêmes. Elles sont répétées à chaque question pour simplifier votre lecture de l'examen.

For the following questions, the T, U & V transactions and the relative order of their transactions are the same. They are repeated with each question to simplify your reading of the exam.

Question 12

Correct

Note de 4,00 sur 4,00

Soit les transactions T, U et V suivantes qui s'exécutent de façon concurrente:

Among the following statements, select the one(s) that are true.

T	U	V
Début		
Lire(A)	Début	
	Lire(B)	
Lire(C)		
	Lire(C)	
	Écrire(B, 4)	
		Début
	Compléter	
Lire(B)		
		Lire(A)
		Écrire(B, 6)
		Écrire(A, 3)
Écrire(A, 2)		
		Compléter
Compléter		

Laquelle ou lesquelles de ces trois transactions pourrai(en)t s'effectuer telle(s) quelle(s), si un contrôle de la concurrence par prise de verrou SANS expiration (partagé pour la lecture et exclusif pour l'écriture) est utilisé?

Which of these three transactions could be done as is, if a lock-based (shared for reading and exclusive for writing) concurrency control WITHOUT expiration is used?

Veuillez choisir au moins une réponse :

- ☐ a. T
- ☒ b. U ✓
- ☐ c. V

Votre réponse est correcte.

- T acquiert le verrou en lecture sur **A** ;
- U acquiert le verrou en lecture sur **B** ;
- T acquiert le verrou en lecture sur **C** ;
- U acquiert le verrou en lecture sur **C** (*partage avec T*) ;
- U promeut son verrou sur **B** en verrou d'écriture ;
- U se complète, et relâche ses verrous sur **B** (*libre*) et **C** (*verrouillé en lecture par T*) ;
- T acquiert le verrou en lecture sur **B** ;
- V acquiert le verrou en lecture sur **A** (*partage avec T*) ;
- V essaie d'obtenir le verrou en écriture sur **B**, mais il ne peut pas à cause de T. S'il abandonne, T peut terminer, mais s'il bloque, T et V vont se bloquer mutuellement car T voudra le verrou en écriture sur **A** que V a pris en lecture.

Avec délai d'expiration des verrous, U et T pourraient terminer. Sans délai d'expiration des verrous, seul U pourrait terminer correctement, T et V étant en interblocage.

La réponse correcte est : U

Soit les transactions T, U et V suivantes qui s'exécutent de façon concurrente:

Among the following statements, select the one(s) that are true.

T	U	V
Début		
Lire(A)	Début	
	Lire(B)	
Lire(C)		
	Lire(C)	
	Écrire(B, 4)	
		Début
	Compléter	
Lire(B)		
		Lire(A)
		Écrire(B, 6)
		Écrire(A, 3)
Écrire(A, 2)		
		Compléter
Compléter		

Laquelle ou lesquelles de ces trois transactions pourrai(en)t être validée(s) si une **validation en avançant** était utilisée pour vérifier la cohérence des transactions ?

Which of these three transactions could be validated if **forward validation** was used to check the consistency of transactions?

Veuillez choisir au moins une réponse :

- ☒ a. T ✓
- ☒ b. U ✓
- ☐ c. V

Votre réponse est correcte.

- U termine en premier, on vérifie ce qu'il a écrit (**B**) et ce que les transactions concurrentes non-terminées ont lu à ce moment (T a lu **A** et **C**, V n'a rien lu) ; **U peut donc compléter**.
- V complète en deuxième, on vérifie ce qu'il a écrit (**A** et **B**) et ce qui a été lu par les transactions concurrentes non-terminées (**A**, **C** et **B** lu par T). Comme T et V intersectent, il y a potentiellement un conflit, et **V doit être abandonnée**.
- T complète en troisième, il n'y a plus de transactions concurrentes non-terminées, et **T peut donc terminer**.

Les réponses correctes sont : T, U

Soit les transactions T, U et V suivantes qui s'exécutent de façon concurrente:

Among the following statements, select the one(s) that are true.

T	U	V
Début		
Lire(A)	Début	
	Lire(B)	
Lire(C)		
	Lire(C)	
	Écrire(B, 4)	
	Compléter	Début
Lire(B)		
		Lire(A)
		Écrire(B, 6)
		Écrire(A, 3)
Écrire(A, 2)		
		Compléter
Compléter		

Laquelle ou lesquelles de ces trois transactions pourrai(en)t être validée(s) si une validation en reculant était utilisée pour vérifier la cohérence des transactions ?

Which of these three transactions could be validated if backward validation was used to check the consistency of transactions?

Veuillez choisir au moins une réponse :

- ☐ a. T
- ☒ b. U ✓
- ☒ c. V ✓

Votre réponse est correcte.

- U termine en premier, il pourra donc compléter sans problème.
- V complète en deuxième, on vérifie ce qu'il a lu (A) et ce qui a été écrit par les transactions terminées (B écrit par U). V et U n'intersectent pas, V peut donc terminer.
- T complète en troisième, on vérifie ce qu'il a lu (A, C, B) et ce qui a été écrit par les transactions terminées (B écrit par U, A et B écrits par V). Comme T et U, ainsi que T et V intersectent, il y a potentiellement un conflit, et T doit être abandonnée.

Les réponses correctes sont : U, V

Question **15**

Terminer

Note de 4,00
sur 4,00

Soit un serveur de temps S utilisé par des drones pour synchroniser leurs horloges et réaliser leur tâche de planter 20 millions d'arbres.

Le drone D envoie un message au serveur S à 13h45m05.100s et reçoit une réponse à 13h45m06.600s. La réponse indique l'heure du serveur S au moment où il a répondu comme étant 13h45m16.040s. En utilisant la méthode de Cristian, calculez le décalage à appliquer à l'heure du drone ainsi que l'intervalle d'incertitude sur cette valeur.

A time server S is used by drones to synchronize their clocks and carry out their task of planting 20 million trees.

The drone D sends a message to the server S at 13h45m05.100s and receives a response at 13h45m06.600s. The response indicates the time of the S server when it responded as 13h45m16.040s. Using Cristian's method, calculate the offset to apply to the time of the drone as well as the range of uncertainty on this value.

On a un temps de réponse à la requête qui est de 1500 ms. On réglera donc l'heure à 13h45m16.040s +0.750s = **13h45m16.790s** avec une incertitude de +/-0.750s.

On a donc un décalage de **10.190s** avec une incertitude de +/-0.750s.

Avec la méthode de Cristian, il suffit de calculer le délai de réponse vu du drone, soit $6.600 - 5.100 = 1.500s$. On assume que cela représente le délai symétrique associé au réseau, et qu'il y a donc $1.500/2 = .750s$ de délai dans chaque direction.

La nouvelle heure sera donc heure du serveur+délai réseau = $13h45m16.040s + .750s = 13h45m16.790s$, de laquelle on soustrait l'heure de réception du message par le drone, soit 13h45m06.600, pour calculer le décalage du drone, soit $10.190 \pm .750$ secondes.

Commentaire :

Question **16**

Terminer

Note de 4,00
sur 4,00

Soit un serveur de temps S utilisé par des drones pour synchroniser leurs horloges et réaliser leur tâche de planter 20 millions d'arbres.

Le drone D envoie un message au serveur S à 13h45m05.100s et reçoit une réponse à 13h45m06.600s. La réponse indique l'heure du serveur S au moment où il a répondu comme étant 13h45m16.040s.

Si le serveur S fournit aussi dans sa réponse l'information comme quoi il a reçu la requête du drone D à 13h45m15.060s, utilisez la méthode de NTP (a, b, ajustement, incertitude, ...) pour calculer le décalage à appliquer à l'heure du drone, ainsi que l'intervalle d'incertitude sur cette valeur.

A time server S is used by drones to synchronize their clocks and carry out their task of planting 20 million trees.

The drone D sends a message to the server S at 13h45m05.100s and receives a response at 13h45m06.600s. The response indicates the time of the S server when it responded as 13h45m16.040s.

If the server S also provided in its response the information that it received the request of the drone D at 13h45m15.060s, use the method of NTP (a, b, adjustment, uncertainty, ...) to calculate the offset to apply to the time of the drone, as well as the range of uncertainty on this value.

$a = 15.060 - 5.100 = 9.960$; $b = 16.040 - 6.600 = 9.440$

decalage = **9.700s** avec un décalage de +/-0.260s

- $a = 15.060 - 5.100 = 9.960$
- $b = 16.040 - 6.600 = 9.440$
- $\text{ajustement} = \frac{a+b}{2} = \frac{9.960+9.440}{2} = \frac{19.400}{2} = 9.700s$
- $\text{incertitude} = \frac{a-b}{2} = \frac{9.960-9.440}{2} = \frac{0.520}{2} = 0.260s$

Le calcul donne donc $9.700 \pm .260$ secondes.

Commentaire :

Soit les évènements suivants se produisant dans 4 drones
déployés pour planter 20 million d'arbres, et qui doivent se
synchroniser ensemble pour ce faire:

The following presents events occurring in 4 drones
deployed to plant 20 million of trees, and having to
synchronize between each other:

Drone D1	Drone D2
1. lecture	1. message Y envoyé à D4
2. écriture	2. écriture
3. message W reçu de D2	3. message W envoyé à D1
4. écriture	4. lecture
5. message X reçu de D3	5. écriture
6. message K envoyé à D2	6. message K reçu de D1
Drone D3	Drone D4
1. écriture	1. lecture
2. message Z reçu de D4	2. message Y reçu de D2
3. lecture	3. écriture
4. message X envoyé à D1	4. message Z envoyé à D3

Afin de comprendre l'ordre relatif des actions qui se
produisent au niveau des drones, et à l'aide des horloges
logiques vous proposez d'associer des vecteurs de
compteurs d'évènements à chaque évènement
($\langle D1, D2, D3, D4 \rangle$).

Complétez le tableau suivant pour indiquer les vecteurs de
compteurs d'évènements associés à chaque évènement
produit dans le système.

In order to understand the relative order of the actions
that occur for the drones, and with the help of the logical
clocks, you propose to associate vectors of event counters
with each event ($\langle D1, D2, D3, D4 \rangle$).

Complete the following table to indicate the event counter
vectors associated with each event produced in the
system.

Drone D1	Drone D2	Drone D3	Drone D4
<div><div>< 1 ✓ , 0 ✓ , 0 ✓ ></div><div>lecture</div></div>	<div><div>< 0 ✓ , 1 ✓ , 0 ✓ ></div><div>message Y envoyé à D4</div></div>		
<div><div>< 2 ✓ , 0 ✓ , 0 ✓ ></div><div>écriture</div></div>	<div><div>< 0 ✓ , 2 ✓ , 0 ✓ ></div><div>écriture</div></div>		
<div><div>< 3 ✓ , 3 ✓ , 0 ✓ ></div><div>message W reçu de D2</div></div>	<div><div>< 0 ✓ , 3 ✓ , 0 ✓ ></div><div>message W envoyé à D1</div></div>		
<div><div>< 4 ✓ , 3 ✓ , 0 ✓ ></div><div>écriture</div></div>	<div><div>< 0 ✓ , 4 ✓ , 0 ✓ ></div><div>lecture</div></div>		
<div><div>< 5 ✓ , 3 ✓ , 4 ✓ ></div><div>message X reçu de D3</div></div>	<div><div>< 0 ✓ , 5 ✓ , 0 ✓ ></div><div>écriture</div></div>		
<div><div>< 6 ✓ , 3 ✓ , 4 ✓ ></div><div>message K envoyé à D2</div></div>	<div><div>< 6 ✓ , 6 ✓ , 4 ✓ ></div><div>message K reçu de D1</div></div>		
<div><div>< 0 ✓ , 0 ✓ , 1 ✓ ></div><div>écriture</div></div>		<div><div>< 0 ✓ , 0 ✓ , 0 ✓ ></div><div>lecture</div></div>	

< 0 ✓, 1 ✓, 2 ✓, 4 ✓ >

message Z reçu de D4

< 0 ✓, 1 ✓, 3 ✓, 4 ✓ >

lecture

< 0 ✓, 1 ✓, 4 ✓, 4 ✓ >

message X envoyé à D1

< 0 ✓, 1 ✓, 0 ✓, 2 ✓ >

message Y reçu de D2

< 0 ✓, 1 ✓, 0 ✓, 3 ✓ >

écriture

< 0 ✓, 1 ✓, 0 ✓, 4 ✓ >

message Z envoyé à D3

Votre réponse est correcte.

La réponse correcte est :

Soit les évènements suivants se produisant dans 4 drones déployés pour planter 20 million d'arbres, et qui doivent se synchroniser ensemble pour ce faire:

The following presents events occuring in 4 drones deployed to plant 20 million of trees, and having to synchronize between each other:

- Drone D1

1. lecture
2. écriture
3. message W reçu de D2
4. écriture
5. message X reçu de D3
6. message K envoyé à D2
- Drone D2

1. message Y envoyé à D4
2. écriture
3. message W envoyé à D1
4. lecture
5. écriture
6. message K reçu de D1
- Drone D3

1. écriture
2. message Z reçu de D4
3. lecture
4. message X envoyé à D1
- Drone D4

1. lecture
2. message Y reçu de D2
3. écriture
4. message Z envoyé à D3

Afin de comprendre l'ordre relatif des actions qui se produisent au niveau des drones, et à l'aide des horloges logiques vous proposez d'associer des vecteurs de compteurs d'évènements à chaque évènement (<D1,D2,D3,D4>).

In order to understand the relative order of the actions that occur for the drones, and with the help of the logical clocks, you propose to associate vectors of event counters with each event (<D1,D2,D3,D4>).

Complétez le tableau suivant pour indiquer les vecteurs de compteurs d'évènements associés à chaque évènement produit dans le système.

Complete the following table to indicate the event counter vectors associated with each event produced in the system.

- Drone D1

<[1],[0],[0],[0]> lecture
<[2],[0],[0],[0]> écriture
<[3],[3],[0],[0]> message W reçu de D2
<[4],[3],[0],[0]> écriture
<[5],[3],[4],[4]> message X reçu de D3
<[6],[3],[4],[4]> message K envoyé à D2
- Drone D2

<[0],[1],[0],[0]> message Y envoyé à D4
<[0],[2],[0],[0]> écriture
<[0],[3],[0],[0]> message W envoyé à D1
<[0],[4],[0],[0]> lecture
<[0],[5],[0],[0]> écriture
<[6],[6],[4],[4]> message K reçu de D1
- Drone D3

<[0],[0],[1],[0]> écriture
<[0],[1],[2],[4]> message Z reçu de D4
<[0],[1],[3],[4]> lecture
<[0],[1],[4],[4]> message X envoyé à D1
- Drone D4

<[0],[0],[0],[1]> lecture
<[0],[1],[0],[2]> message Y reçu de D2
<[0],[1],[0],[3]> écriture
<[0],[1],[0],[4]> message Z envoyé à D3

Question **18**

Terminer

Note de 10,00
sur 12,00

Vous devez planifier un nouveau centre de données et comparer différents scénarios. Vous avez déjà prévu examiner la performance des systèmes (et les revenus qu'on peut en tirer), le coût des ordinateurs, le coût du bâtiment ainsi que les coûts d'opération et de renouvellement des équipements, afin de déterminer le projet le plus rentable sur la durée de vie anticipée.

Devez-vous comme ingénieur aussi vérifier les aspects du développement durable de ce projet? Justifiez votre réponse en développant les trois points suivants:

1. Quelles sont les lois applicables?
2. Quelles sont les différentes phases du cycle de vie?
3. Quels sont les quatre différents types d'impact sur l'environnement?

You need to plan a new data center and compare different scenarios. You have already planned to examine the performance of the systems (and the revenues that can be derived from them), the cost of the computers, the cost of the building as well as the costs of operation and renewal of the equipment, in order to determine the project the most profitable over the anticipated life.

Do you, as an engineer, also check the sustainability aspects of this project? Justify your answer by developing the following three points:

1. What are the applicable laws?
2. What are the different phases of the life cycle?
3. What are the four different types of environmental impact?

Oui, en tant qu'ingénieur, je dois également vérifier les aspects de développement durable de ce projet. Les lois applicables sont: la loi du Québec de 2006 sur le développement durable, la loi du Canada de 2008 sur le développement durable, le code de déontologie de l'Ordre des Ingénieurs du Québec (BAPE pas applicable pour centre de données). Toutes les phases du cycle de vie qui doivent être prises en compte lors de cette vérification, à savoir: la fabrication, le transport, l'opération du site (consommation énergétique, etc) et la fin de vie (qui inclut le recyclage des différents matériaux et la disposition qui sera faite des locaux). Les types d'impact sur l'environnement sont l'impact sur: la santé humaine, l'écologie, les changements climatiques et l'épuisement des ressources.

L'ingénieur doit tenir compte des conséquences de l'exécution de ses travaux sur l'environnement dans une perspective de développement durable.

1. Ceci est prescrit par la loi canadienne de 2008 sur le développement durable, la loi québécoise de 2006 sur le développement durable, et le code de déontologie de l'Ordre des Ingénieurs du Québec. La procédure d'évaluation environnementale du BAPE ne s'applique normalement pas à un centre de données.
2. Les phases du cycle de vie sont la fabrication (construction du site et fabrication des équipements), le transport (des matériaux pour la construction et des équipements), l'opération du site (entretien, alimentation électrique...) et finalement la fin de vie (la démolition ou conversion du bâtiment, la restauration du site, et le recyclage ou la mise aux rebuts des matériaux et équipements).
3. Pour toutes les activités qui se retrouvent dans ces différentes phases, il faut examiner l'impact sur la santé humaine, sur l'écologie, sur les changements climatiques et sur l'appauvrissement des ressources. Pour un centre de données typique, une grande partie de l'impact est reliée à la consommation d'énergie pendant l'opération de l'équipement informatique et de la climatisation. Un autre impact non négligeable est la fabrication des équipements informatiques et électriques, en particulier le raffinage de l'or et du cuivre requis pour ces équipements.

Etant donné l'importance de la consommation électrique, une source d'énergie propre, et un climat froid qui ne requiert pas de climatisation, peuvent diminuer considérablement l'impact négatif d'un centre de données.

Commentaire :

4/4

3/4

3/4