E5SR : PRODUCTION ET FOURNITURE DE SERVICES

Durée : 4 heures **Coefficient : 5**

CAS HTS

ÉLÉMENTS DE CORRIGÉ

Barème

Partie A	**50**
Mission 1	37,5
Mission 2	12,5
Partie B	**50**
Mission 1	22,5
Mission 2	7,5
Mission 3	20
Total	**100**

Les parties en italique représentent des exemples de réponses aux questions posées pouvant aller au-delà des réponses attendues pour un candidat. Elles n'ont aucun caractère d'exhaustivité et il appartient à chaque correcteur d'évaluer la cohérence de toute autre proposition.

Partie A – Conseil avant-vente au client *Bloom*

Mission 1 : préparation de la présentation d'une solution d'infrastructure

Question A.1.1
Préparer des éléments de réponse convaincants aux questions techniques posées par les responsables de *Bloom* et en particulier par ceux qui travaillent au siège de Pannes-en-Argonne.

a. « Si le coup de pelleteuse se reproduit, comme la dernière fois, au même endroit je ne vois pas ce qui va changer. »
b. « Chaque fois qu'on recevra de nouvelles versions de l'ERP, va-t-il falloir se déplacer pour les installer ? »
c. « Expliquez-moi comment vous garantissez que notre trafic réseau sera séparé de celui des autres clients ? »
d. « Quel dispositif mettez-vous en place pour la sauvegarde de nos données métier ? »
e. « Quel est l'intérêt du serveur *proxy* que vous voulez nous louer ? Pourquoi centraliser la sortie de nos postes sur Internet ?»
f. « Pourquoi répartir nos serveurs de *mail* et *web* dans une DMZ publique, notre serveur ERP dans une autre DMZ privée, et nos autres serveurs dans notre VLAN dédié ? »

Réponse A.1.1.a

« Si, cela change beaucoup de choses ! Le coup de pelleteuse coupera la liaison entre le siège et les serveurs centraux, mais pas celles entre les serveurs centraux et les autres sites, et notamment, l'accès des boutiques et de l'internet public. Une grande partie du système continuera de fonctionner, mais en mode dégradé, sans alimentation de données à partir du siège (de l'usine notamment). »

Réponse A.1.1.b

« Non, vous disposerez d'un d'accès distant sécurisé aux serveurs centralisés et pourrez même les allumer à distance, via le système ILO. Les mises à jour de l'ERP se feront de cette manière, sans vous déplacer. »

Réponse A.1.1.c

« Nous le garantissons par une séparation logique des réseaux de chacun de clients, par la technologie des VLAN. Chaque client voit ses machines placées dans un VLAN qui lui est strictement propre, avec son propre plan d'adressage IP, si besoin. ».

Réponse A.1.1.d

« Les sauvegardes sont automatisées. Elles sont effectuées à partir d'un VLAN connectant toutes les systèmes à sauvegarder sur une prise Ethernet dédiée de chacune des machines. Les données sont sauvegardées à la fois sur disque et sur bande avec placement en armoire forte. »

Réponse A.1.1.e

« La sortie sur L'internet via un seul accès unique centralisé permet de mieux contrôler cette sortie. En l'occurrence, on pourra utiliser le serveur proxy dans différents rôles : du filtrage (sites web en liste blanche ou noire, filtrage horaire, etc.), de la priorisation, de la lutte antivirale, antispam, etc. »

Réponse A.1.1.f

« Cette répartition VLAN Client / DMZ publique / DMZ privée offre les meilleures garanties de sécurité anti-intrusion. Le serveur web, qui est le plus exposé, se trouve dans un premier sas, il aura le droit d'échanger des informations avec le serveur ERP, mais pas avec le reste des serveurs du client Bloom. Le serveur ERP pourra échanger des informations avec les serveurs du VLAN du client, notamment depuis les machines TSE qui font tourner les applications « métiers » du client Bloom. »

Question A.1.2
Rédiger les réponses suivantes de la FAQ présentant les avantages, pour un client, de faire héberger ses serveurs au sein de la ferme *Hebertek* quelle que soit la solution d'hébergement retenue :

a. Sur le plan de la disponibilité des communications vers les serveurs hébergés ;
b. Sur le plan de la sécurité physique des serveurs ;
c. Sur le plan financier ;
d. Sur le plan de l'évolutivité de l'infrastructure du système informatique du client ;
e. Sur le plan humain et des différentes responsabilités entre le client et *Hebertek*.

Réponse A.1.2.a

La ferme de serveurs Herbertek est « alimentée » par quatre FAI de FAI différents, offrant un haut niveau de garantie. Il y a très peu de risque que la ferme soit coupée de l'Internet.

Réponse A.1.2.b

La sécurité physique des serveurs est assurée par une batterie d'équipements spécialisés : climatisation, onduleurs, générateurs électriques, protection anti-incendie, protection anti-intrusion avec accès sécurisé par badge, redondances diverses sur les machines : des alimentations, disques RAID, des liens SAN, etc.

Réponse A.1.2.c

Au plan financier, l'hébergement en location de puissance et l'infogérance permettront de ramener tout ou partie du coût de l'informatique à une facture mensuelle d'un montant contractualisé. L'hébergement simple ne dispensera pas d'acheter et d'amortir les équipements.

Réponse A.1.2.d

Dans le cas de l'hébergement en location de puissance, l'évolutivité du système d'information est garantie par le fait que les machines et les liens sont dimensionnés de manière contractualisée. L'augmentation de leurs performances et fonctionnalités passera par une simple révision des termes du contrat. Les ajustements techniques (mémoire, CPU, débit des liens, etc.) seront du ressort de l'hébergeur.

Réponse A.1.2.e

Le problème des ressources humaines liées à l'infrastructure (essentiellement disponibilité d'un personnel qualifié) est du domaine de l'hébergeur et plus celui du client. Le client pourra donc bénéficier de l'expertise des différents spécialistes de la société HTS sans pour autant devoir embaucher tel ou tel spécialiste. Les responsabilités de chacune des parties seront clairement définies dans le contrat d'hébergement.

Question A.1.3
Justifier l'utilisation du protocole VTP dans le cadre de l'architecture proposée par *Hebertek*.

Réponse A.1.3

L'usage du protocole VTP (ou d'un autre protocole non propriétaire comme GVRP) a pour but de simplifier la gestion des VLAN dans des réseaux importants.

Normalement pour ajouter un VLAN sur un réseau, l'administrateur doit l'ajouter sur chaque commutateur. Pour éviter cela, sur des commutateurs Cisco, la manipulation peut être faite sur un seul commutateur. La modification est alors diffusée sur les autres via le protocole VTP (VLAN Trunking Protocol). On distingue dans ce cas, des commutateurs VTP server et des VTP client. Le VTP server va diffuser la modification vers les commutateurs VTP client qui appartiennent au même domaine que lui.

Le VLAN 195 sera créé dans le commutateur serveur. Il se diffusera alors dans tous les commutateurs du même domaine.

Le nombre de VLAN à gérer et le nombre de commutateurs de l'infrastructure réseau d'Hebertek, justifie totalement l'utilisation du protocole VTP.

Mission 2 : évaluation d'un risque lié à la fourniture d'un service

Question A.2.1
Expliquer en quoi consiste une attaque par déni de services (DOS).

Réponse A.2.1

Le Denial-of-service ou déni de service est une attaque visant à rendre muette une machine en la submergeant de trafic inutile. Il peut y avoir plusieurs machines à l'origine de cette attaque (c'est alors une attaque distribuée : DDoS) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter.

Un serveur victime d'une attaque de type "DoS" va ralentir (dans le meilleur des cas), redémarrer (plantage), ou ouvrir un accès à l'attaquant (dans le pire des cas). Il y aura donc dégradation du service, voir une interruption de celui-ci.

Un site web de commerce électronique ne pourra pas répondre aux demandes des clients, avec de lourdes conséquences en termes de perte financière, de dégradation de l'image de marque et de la confiance accordée par les clients.

Question A.2.2
Citer les commandes de l'outil de supervision qui permettront d'alerter au plus tôt en cas de nouvelle attaque sur le site *web* et justifier leur usage dans le cas d'une attaque par déni de service (DOS).

Réponse A.2.2

Suite à l'analyse du document 2.2 « L'outil de supervision », pour vérifier la bonne santé d'un serveur web, il faut surveiller le trafic, les temps de réponse, le nombre de processus actifs, si l'hôte répond et les temps de réponse du ping.

Les alertes permettront de savoir s'il y a un nombre de connexions trop important par rapport à la consultation normale, ou trop de processus ouverts.

Elles permettront aussi de savoir si le serveur web répond dans des délais corrects tant au niveau du ping que du temps de réponse du site web.

Partie B – Mise en place et maintenance du nouveau réseau *Bloom*

Mission 1 : mise à jour des réseaux des sites de la société *Bloom*

Question B.1.1
Justifier le bien fondé de la proposition de l'administrateur réseau *d'Hebertek* de supprimer la ligne 4 de la table de routage de cet équipement.

Réponse B.1.1

	réseau	Masque	passerelle	interface
Route statique	10.16.0.0	255.255.0.0	192.168.0.2	192.168.0.1

Cette ligne a été configurée manuellement (statique) afin d'apprendre au routeur RBL la route vers le réseau de Pannes-en-Argonnes (10.16.0.0). Le trafic destiné au réseau 10.16.0.0 est envoyé à la passerelle 192.168.0.2, c'est-à-dire le routeur SDSL. ***Mais en fait cette ligne est déjà comprise dans la ligne 5 qui est la route par défaut ; elle est donc inutile.***

Cette ligne n'a par ailleurs plus d'utilité dans la nouvelle architecture parce que les routes sont modifiées suite au déplacement des serveurs.

Question B.1.2
Donner toutes les modifications de configuration à réaliser sur ce commutateur-routeur pour obtenir le fonctionnement attendu dans la nouvelle configuration du réseau de la société *Bloom*.

Réponse B.1.2

Il faut remplacer l'adresse de l'interface 192.168.0.1 par l'adresse 172.22.0.253

Il faut créer le VLAN 4 dans le routeur RBL et lui affecter l'adresse IP qui servira d'adresse de passerelle aux caméras IP

N° de VLAN	*Réseau*	*Adresse de l'interface*
4	*Caméras IP*	*192.168.2.126/27*

Cette opération ajoute automatiquement la route connectée vers le réseau des caméras :

	réseau	*Masque*	*passerelle*	*interface*
Route connectée	*192.168.2.96*	*255.255.255.224*	*192.168.2.126*	*192.168.2.126*

Il faut modifier la route par défaut en tenant compte de la nouvelle passerelle HBP :

Réseau	***Masque***	***passerelle***	***interface***
0.0.0.0	*0.0.0.0*	*172.22.0.254*	*172.22.0.253*

Il faut activer le protocole RIP et publier les réseaux locaux qui font partie du sur-réseau 192.168.2.0/24 et le réseau de liaison avec le routeur de terminaison 172.22.0.0

router rip	*Mise en route du protocole de routage RIP*
network 172.22.0.0	*Indication du réseau de liaison directement connecté*
network 192.168.2.0	*Indication du sur-réseau englobant les 3 VLANs*

Question B.1.3
Expliquer si le basculement de l'ancienne configuration de ce matériel vers la nouvelle provoquera une interruption de service.

Réponse B.1.3

Si le routeur RBL a suffisamment de ports pour pouvoir configurer la connexion vers HBP sans déconnecter le réseau actuel vers SDSL alors l'interruption de service pourra être évitée, tout comme si on effectue les nouveaux réglages dans un routeur équivalent de test et qu'on fait une sauvegarde du fichier de configuration en utilisant éventuellement un serveur TFTP.

Toutefois au moment du basculement les connexions en cours seront perdues. Il est donc préférable de ne pas faire la migration pendant les heures de travail.

Mission 2 : configuration du serveur d'application

Question B.2.1
Justifier le fait que le mode de répartition choisi par *Hebertek* pour le client *Bloom* soit le mode de répartition de charge **«** Répartition égale » du RCR.

Réponse B.2.1

La répartition prioritaire n'est pas le mode le plus adapté car il s'agit d'un mode gérant uniquement la tolérance de panne (si un serveur est en panne un autre prend le relais). Donc cela n'augmente pas le nombre de sessions disponibles.

Vu que les serveurs rajoutés dans la grappe possèdent des caractéristiques physiques identiques le mode de « répartition égale » est ici le plus approprié. Les connexions initiales seront réparties équitablement entre les trois serveurs de la grappe ce qui plus performant que le mode de répartition manuel.

Mission 3 : maintenance du serveur d'application

Question B.3.1
Rechercher les causes du dysfonctionnement et alimenter la base de connaissance en expliquant dans une courte note l'origine de cet incident et la solution à mettre en œuvre pour y remédier.

Réponse B.3.1

La répartition de charge réseau RCR en mode de répartition égale se charge uniquement de distribuer uniformément les requêtes arrivant sur les serveurs. Il se peut très bien que des utilisateurs restent connectés sur une session très longtemps sur un des serveurs tandis que d'autres se déconnectent au bout de cinq minutes sur un autre. Cela va forcément, au bout d'un certain temps, créer un déséquilibre au niveau du nombre de sessions ouvertes sur les différents serveurs. Car le protocole RCR ne regarde pas le taux d'occupation des ressources des serveurs, il se contente de ***rediriger les requêtes réseaux****.*

Pour éviter ce problème il faut donc installer un protocole supplémentaire qui tienne compte du nombre de sessions ouvertes sur chaque serveur. Il s'agit du protocole ES (équilibrage de sessions) décrit dans le document 5.2 Répartition de charge réseau / équilibrage de sessions Terminal Serveur

Question B.3.2
a. Expliquer les causes de l'apparition de ce message.

b. Écrire les procédures pour résoudre cet incident.

(Extrait de http://www.reseaucerta.org/docs/cotelabo/coteLaboServiceWeb.pdf)

Réponse B.3.2a

Lorsque vous vous connectez à un site web sécurisé, le serveur hébergeant ce site présente à votre navigateur un "certificat" afin de vérifier l'identité du site. Ce certificat contient des informations d'identité, telles que l'adresse du site web, laquelle est vérifiée par un tiers approuvé par votre ordinateur. En vérifiant que l'adresse du certificat correspond à l'adresse du site web, il est possible de s'assurer que vous êtes connecté de façon sécurisée avec le site web souhaité et non pas avec un tiers (tel qu'un pirate informatique sur votre réseau).
Ce certificat doit donc être vérifié par un tiers approuvé c'est à dire reconnu par votre ordinateur.

Cette alerte de sécurité veut dire que le certificat n'a pas été émis par un tiers connu. Cette situation est ici normale car la société Bloom n'a pas eu recours à un tiers de confiance mais a généré son propre certificat.

Le problème se produit de la même manière pour chacun des serveurs TSE.

Réponse B.3.2b

Pour résoudre ce problème en toute sécurité, il faut soit importer le certificat racine de l'entreprise en tant que "certificat racine" dans le navigateur des postes des boutiques (le certificat doit apparaître dans la liste des certificats des autorités principales de confiance), soit acheter le certificat du site web auprès d'une autorité de certification mondialement reconnue. Ces solutions font disparaitre le problème.

On peut aussi décider de toujours faire confiance à ce certificat pour les prochaines sessions, mais cette solution est moins propre.