CAS CM'IN

ÉLÉMENTS DE CORRIGÉ

Les éléments en italique sont des éléments de compréhension, des compléments ou des explications, non exigés dans la réponse du candidat.

Barème

Partie A	*Gestion des clients du MAN*	50 points
Partie B	*Projets internes à CM'IN*	50 points
	Total	100 points

Dossier A

Mission 1

Question A.1.1
Proposer des réponses argumentées aux trois interrogations posées par monsieur Poulin dans l'entretien retranscrit dans le dossier documentaire.

La documentation spécifique au dossier A (documents 2, 3 et 4) oriente la réponse vers le 802.1Q et le 802.1ad. D'autres réponses cohérentes (notamment une argumentation sur la fibre noire) peuvent néanmoins être envisagées pour répondre à ce questionnement de départ, le Q in Q n'étant pas explicitement cité dans l'entretien.

- **Vos autres clients peuvent-ils capturer les trames liées à notre communication inter-sites circulant sur votre réseau optique ?**

Tous nos clients utilisant notre réseau sont isolés dans un VLAN spécifique. En l'occurrence pour votre société vous avez l'id de vlan 174. Notre réseau étant de type Ethernet les liaisons physiques fibres formant notre backbone sont mutualisées (niveau 1) mais les trames circulant sur celles-ci sont tagguées via le protocole 802.1Q et sont donc totalement isolées de celles des autres clients (niveau 2).
La réponse doit mettre en valeur l'aspect isolant et donc sécurisant d'un vlan en expliquant l'intérêt du tag sur la partie liaisons mutualisées.
La réponse peut également expliquer l'isolation grâce à la fibre noire.

- **Pourrons-nous tagguer nos trames et ainsi faire communiquer nos VLAN 50 et 100 présents aux sièges avec d'autres postes sur ces mêmes VLAN du bâtiment de Luce ?**

Tout à fait, nous utilisons la technologie 802.1ad plus communément appelé Q in Q ou Vlan Stacking, cela consiste à ajouter un second tag à la trame Ethernet.

Les numéros des VLAN que vous utilisez resteront exactement les mêmes et seront retransmis comme ce serait le cas par une liaison 802.1Q.

Pour résumer, il y a un premier Tag correspondant à votre identifiant client au sein de notre réseau (ici le vlan 174) et un second Tag correspond à l'identifiant de VLAN pour laquelle la trame est destinée au sein de votre réseau (vos VLANs 50 et 100).

La réponse doit mettre en valeur l'aspect de double tag dans l'objectif de répondre à l'interrogation du client.
La réponse peut également expliquer l'utilisation de VLAN possible sur la fibre noire.

- **Les échanges de données sont-ils sécurisés comme dans un VPN site à site de type IPSEC ?**

IPSec est un protocole sécurisé qui fonctionne au niveau 3 du modèle OSI, cela signifie qu'il faut faire du routage. Dans votre cas nous fonctionnons au niveau 2, et vous êtes sur notre réseau opérateur. Cela signifie que les trames ne circulent pas sur le réseau public.

La couche cryptographique n'est donc pas nécessaire car nous garantissons la confidentialité des échanges sur notre réseau physique via nos VLAN clients spécifiques à chacun de nos clients.
Vous aurez ainsi un réseau bien plus performant et pourrez profiter de toute la bande passante que nous vous proposons avec un débit garanti.

La réponse doit mettre en valeur que la solution mise en place (niveau 2 OSI) n'intègre pas

nécessairement de chiffrement car la transmission des données ne s'effectue pas sur un réseau public. La réponse pourra également préciser qu'il est quand même préférable de chiffrer les échanges car la solution repose ici sur une certaine confiance vis-à-vis de l'opérateur.

Question A.1.2
Indiquer, dans un tableau comparatif, au moins un avantage et un inconvénient pour chaque solution proposée (connexion fibre noire et *LAN2LAN*) par CM'IN à son client GPF.

	Lan to Lan	**Fibre noire**
Avantages	Equivalent à une liaison 802.1Q entre site distant. Facturation spécifique pour cette offre Paramétrage et configuration par l'opérateur (CM'IN) Equipements souvent compris dans l'abonnement Prestation clé en main, pas de travaux d'installation.	Totalement sécurisée dans le sens où on a une isolation physique. Liaison Point à Point (dédiée) entre les deux bâtiments Contrôle total de l'architecture du réseau (par le client) Choix des équipements de raccordement libre car le client en sera le propriétaire Pas d'abonnement Coût intéressant sur courte distance (300 € pour 300m)
Inconvénients	Complexe à mettre en place sans un prestataire. Nécessite des équipements spécifiques (solution captive) : commutateurs Metropolitains (mis en place par l'opérateur) Perte de maitrise de l'infrastructure	Facturation à la distance ➢ Tarif trop élevé pour une connexion directe avec le siège et Lucé (15 km = 15 000 €) Nécessite des compétences locales pour le raccordement et la configuration Autre élément de coût : nécessité d'acheter les équipements.

Question A.1.3
Indiquer quelles sont les conséquences – à court terme et à plus long terme – de l'annonce de l'arrêt de la commercialisation de l'équipement pour CM'IN.

CM'IN n'a pas d'urgence à court terme de changer ces équipements car ils sont encore maintenus jusqu'au 4/1/2022 (pour ce qui concerne la partie mises à jour de sécurité).

L'arrêt de la commercialisation du modèle CISCO ME 3400 va entrainer pour CMIN la nécessité de prévoir d'investir à moyen terme dans de nouveaux équipements.
Il faudra vérifier et mettre à jour éventuellement les équipements avant le 04 janvier 2022

Si CM'IN dispose d'un contrat de maintenance auprès de CISCO, elle pourra selon le cas faire réparer ses équipements mais plus aucune mise à jour du *firmware* ne sera proposée, les équipements seraient donc potentiellement vulnérables à une faille pour laquelle aucun patch ne sera disponible.

Autre solution possible :

La migration va prendre du temps :

- *Inventaire des équipements à changer*
- *Choisir le nouvel équipement (pas forcément de CISCO puisqu'il n'y a pas de produit de remplacement), compatible avec les technologies nécessaires à savoir : MPLS, Q in Q*
- *Effectuer des tests*
- *Configuration et déploiement adapté à chaque client (commutateur de démarcation)*
- *Remplacement des équipements*
- *Retour des équipements et gestion de leur mise au rebus.*

Tant que les équipements sont fonctionnels et qu'aucune faille de sécurité n'est découverte sur ces produits, on garde les équipements en place.
Il faut toutefois trouver un équipement de remplacement pour les futurs clients ce qui entrainera un parc d'équipements hétérogène.
Cela permet de réduire le coût en comparaison à un changement de tous les équipements utilisés.

Mission 2

Question A.2.1
Indiquer en le justifiant, combien d'adresse(s) IP publique(s) doivent être allouée(s) à un client *CM'IN Box*.

Les clients *CM'IN Box* obtiennent une IP dans l'intervalle qui leur est réservé.
1 client = 1 IP publique.

Question A.2.2
Proposer un numéro de réseau local virtuel (*VLAN*) et un réseau IP (avec le masque) répondant à ce besoin.

Le VLAN attendu est le n° 175 (d'après le document 10) : il fait suite au n° du dernier client enregistré

Avec un /29 cela fournirait $2^3 = 8$ adresses IP publiques pour le client. ⇨ Insuffisant.
Il faut donc un réseau avec un **masque en /28 (255.255.255.240)**

Le dernier client (GPF) a un réseau IP allant jusqu'à l'adresse IP 87.28.138.223
223 correspond à **1101** 1111

La plage suivante en /28 commence à 224 sur le 4ème octet
Avec **1110** 0000 = 224
*La plage IP de ce réseau ira de l'adresse réseau **87.28.138.224** jusqu'à l'adresse IP de diffusion 87.28.138.239. Ce réseau permet d'avoir 14 adresses, donc les 10 adresses IP souhaitées.*

Question A.2.3
a) Indiquer dans une note à votre responsable quels sont les risques d'une gestion des adresses IP par l'outil actuel.
b) Indiquer les avantages à utiliser la solution IPAM* pour ce besoin de gestion des adresses IP.

a) La gestion des IP (surtout des IP publiques) est critique car le nombre d'adresses est limité. Elles doivent évidemment rester uniques sur le réseau. CM'IN a la responsabilité d'attribuer les IP publiques à ses clients et ne peut pas se permettre de faire des erreurs.
Utiliser un tableur pour gérer ce genre de données est mal adapté car le fichier s'il n'est pas centralisé peut se retrouver dans plusieurs versions différentes (lequel est le bon ?). Cela risque d'entrainer des erreurs d'attribution / configuration.
Il est indispensable de centraliser la gestion des IP au sein du système d'information et mettre en place un système d'habilitation pour les opérations d'ajout / suppression / modification à des utilisateurs parfaitement authentifiés. Une solution multiutilisateur reposant sur une base de données unique est le minimum.
On peut également soulever la problématique des risques sur le plan juridique.
En effet, la responsabilité des liens IP publique – client est très importante en cas d'enquêtes judiciaires. L'opérateur doit pouvoir permettre à la justice de remonter jusqu'au client avec certitude et preuve.

b) IPAM a de nombreux avantages :
- centralisation des affectations IP par client
- traçabilité des adresses IP
- optimisation de l'utilisation et des capacités des services DHCP et DNS
- peut-être aussi un avantage sécurité : la feuille Excel peut être plus accessible

Question A.2.4
Pour la solution S1
a) Indiquer les adresses des deux réseaux IP obtenus (offre FTTH* mutualisée) ainsi que l'adresse des passerelles correspondantes.
b) Détailler les modifications à effectuer sur la configuration du service DHCP.

a)
On scinde le réseau initial en 2 donc 1 seul bit est nécessaire. On passe donc de /21 en /22.
A l'origine :

Adresses réseau (déc.)	**46**	**11**	**128**	**0**
Masque (déc.)	**255**	**255**	**248**	**0**
Adresses réseau (bin.)	**0010 1110**	**0000 1011**	**1000 0000**	**0000 0000**
Masque (bin.)	**1111 1111**	**1111 1111**	**1111 1000**	**0000 0000**
Adresse diffusion (bin.)	**0010 1110**	**0000 1011**	**1000 0111**	**1111 1111**
Adresse diffusion (déc.)	**46**	**11**	**135**	**255**

Après scindement :

Premier réseau

Adresses réseau (déc.)	**46**	**11**	**128**	**0**
Masque (déc.)	**255**	**255**	**252**	**0**
Adresses réseau (bin.)	**0010 1110**	**0000 1011**	**1000 0000**	**0000 0000**
Masque (bin.)	**1111 1111**	**1111 1111**	**1111 1100**	**0000 0000**
Adresse diffusion (bin.)	**0010 1110**	**0000 1011**	**1000 0011**	**1111 1111**
Adresse diffusion (déc.)	**46**	**11**	**131**	**255**

Deuxième réseau

Adresses réseau (déc.)	**46**	**11**	**132**	**0**
Masque (déc.)	**255**	**255**	**252**	**0**
Adresses réseau (bin.)	**0010 1110**	**0000 1011**	**1000 0100**	**0000 0000**
Masque (bin.)	**1111 1111**	**1111 1111**	**1111 1100**	**0000 0000**
Adresse diffusion (bin.)	**0010 1110**	**0000 1011**	**1000 0111**	**1111 1111**
Adresse diffusion (déc.)	**46**	**11**	**135**	**255**

La passerelle étant la dernière IP disponible sur le réseau IP on obtient :

VLAN	Client ou Service	Réseau IP	Equipement interface Gateway	Passerelle
4000	FTTH-Mutualise	46.11.128.0 /22	NetCenter	46.11.131.254
4001		46.11.132.0 /22	TelHouse2	46.11.135.254

A noter : Il faudra reconfigurer l'interface du routeur de TelHouse2 sur le VLAN 4001. (non demandé)

b) Détailler les modifications à effectuer sur la configuration du service DHCP.

NRO/PoP Lucé	NRO/PoP Gellainville
*inet 46.11.128.1 netmask 255.255.**252**.0 broadcast 46.11.**131.255***	*inet 46.11.135.253 netmask 255.255.**252**.0 broadcast 46.11.135.255*

# fichier /etc/dhcp/dhcpd.conf 	
 	
#Serveurs DNS
option domain-name-servers 46.11.128.1, 46.11.135.253;
 	
#Passerelle des box (NetCenter)
option routers 46.11.**131.254;**
 	
#Durée du bail en secondes
default-lease-time 604800; # 7 jours
max-lease-time 950400; # 11 jours
 	
# étendue adresses 1 	
subnet 46.11.128.0 netmask 255.255.**252**.0 {
range 46.11.128.2 46.11.131.**253**;
}
	# fichier /etc/dhcp/dhcpd.conf
	
	#Serveurs DNS
	option domain-name-servers 46.11.135.253, 46.11.128.1;
	
	#Passerelle des box (TelHouse)
	option routers 46.11.135.254;
	
	#Durée du bail en secondes
	default-lease-time 604800; # 7 jours
	max-lease-time 950400; # 11 jours
	
	# étendue adresses 2
	subnet 46.11.**132**.0 netmask 255.255.**252**.0 {
	range 46.11.**132.1** 46.11.135.252;
	}

Question A.2.5
Pour la solution S2

a) Indiquer s'il est possible de répartir la charge sur les deux routeurs en modifiant uniquement la configuration initiale des serveurs DHCP et en ne gardant qu'un seul réseau local virtuel (*VLAN*). *Vous proposerez si nécessaire une modification de la configuration.*
b) Expliquer pourquoi les boitiers (*box*) des clients situés à l'est de Chartres recevront probablement leur configuration de la part du serveur DHCP de Gellainville et les clients de l'ouest la recevront du serveur de Lucé.

a)
Les 2 plages d'adresses IP sont sur le même VLAN ce qui implique qu'ils sont sur le même domaine de diffusion. Cela permet en cas de défaillance d'un des serveurs DHCP que le second soit capable de répondre.

Il y avait déjà deux serveurs DHCP (non clustérisés) avec deux plages distinctes à peu près similaires mais qui distribuaient la même passerelle à l'ensemble des clients d'où la saturation du routeur.

Il suffit donc de changer uniquement l'adresse de la passerelle dans la configuration DHCP pour que les clients se répartissent sur les 2 routeurs

NRO/PoP Lucé	NRO/PoP Gellainville

option routers 46.11.128.**2;**
#première adresse disponible après le serveur DHCP
 	
subnet 46.11.128.0 netmask 255.255.248.0 {
range 46.11.128.**3** 46.11.131.255;
}
	option routers 46.11.135.254;
	
	subnet 46.11.128.0 netmask 255.255.248.0 {
	range 46.11.132.0 46.11.135.252;
	}

Cela permet de libérer 2 adresses (@IP de réseau et @IP de diffusion du 2ieme VLAN)

Il n'y a pas de solution unique, toute configuration pertinente est acceptée, notamment l'avant-dernière adresse de la plage (46.11.135.253) pour le routeur se trouvant dans le NRO/Pop de Lucé.
Les plages distribuées doivent être en cohérence avec le choix du routeur.

b)
Quand les serveurs sont dans le même VLAN, un client DHCP prend (généralement) la première offre IP qu'il reçoit, en conséquence, il est fort probable que la répartition se fasse comme suit :

Chaque serveur DHCP répondra aux clients qui sont les plus proches, ainsi les clients raccordés aux NRO de Dreux et de Lucé devraient obtenir leurs IP du serveur DHCP1 du NRO de Lucé (à l'ouest).

Les clients raccordés au NRO de Gellainville et d'Epernon devraient obtenir une IP distribuée par le serveur DHCP2 de Gellainville (à l'est).

De plus l'anneau optique a un lien désactivé par le protocole STP entre le NRO de Epernon et celui de Lucé, ce qui rend l'un des serveurs DHCP beaucoup plus « éloigné » des clients *(nombre d'équipements intermédiaires important)*.

Question A.2.6
Expliquer la raison pour laquelle les adresses des serveurs DNS ne sont pas fournies dans le même ordre dans la configuration des serveurs DHCP.

L'ordre a une importance dans la partie options DNS. Le client DHCP interroge toujours en premier le serveur DNS qui se trouve en premier paramètre. Le serveur DNS se trouvant en deuxième paramètre n'est sollicité par le client uniquement lorsque le serveur 1 n'est pas joignable.

L'inversion des paramètres permet de répartir les requêtes de l'ensemble des clients DHCP tout en maintenant une disponibilité sur l'ensemble des clients DHCP.

Autre justification possible : On donne à chaque client l'adresse du DNS « le plus proche » géographiquement, ce qui devrait accélérer les échanges DNS.

Dossier B – Projets internes à CM'IN

Mission B.1 – Gestion des comptes des utilisateurs de CM'IN

Question B.1.1
Expliquer les risques liés à la non-suppression de ces comptes.

- Des comptes restés activés pourraient être utilisés à des fins malveillantes. *Il est important de supprimer ou de désactiver les comptes d'utilisateurs ayant quitté l'entreprise (stagiaires, intérimaires, prestataires).*
- Encombrement de la base de données

Question B.1.2
Expliquer pourquoi la suppression ne peut pas être complètement automatique.
Vous justifierez votre réponse en donnant un exemple concret.

Il convient de lister régulièrement, par exemple tous les mois, les comptes non utilisés. Il faut ensuite décider si ces comptes doivent être supprimés ou seulement désactivés. Aucune procédure automatique n'est acceptable car il peut y avoir des cas où les comptes non utilisés doivent être conservés (congé, congé maladie, congé maternité, déplacement / mission longue chez un client, etc.).

D'autres raisons peuvent être invoquées : par exemple l'accès aux données d'un utilisateur qui pourrait être rendu difficile voire impossible (données cryptées).

Question B.1.3
Indiquer la modification à effectuer dans le *script* pour lister uniquement les comptes désactivés.

```
# import du module active directory
Import-Module ActiveDirectory

# liste des comptes utilisateurs désactivés avec la date de leur dernière connexion
# et export du resultat vers le fichier ListeUser.csv
$ListeUser= Get-ADUser -Filter {enabled -eq $false} -Properties LastLogonDate | export-csv c:\ListeUsersDesactives.csv
```

Remarque : L'utilisation des variables prédéfinies est préférable, mais l'écriture {enabled -eq "false"} fonctionne. Idem pour l'écriture {enabled -ne $true} ou {enabled -ne "true"}

Question B.1.4
En vous aidant de la documentation fournie, compléter l'ébauche du script proposé qui permettra de lister les comptes activés mais inutilisés depuis plus de 30 jours.

```
# import du module active directory
Import-Module ActiveDirectory

# Calcul date inactivite
# Nombre de jours inactivite
$JourInactivite = 30

# On retire 30 jours à la date du jour
$Limite = (Get-Date).Adddays(-$JourInactivite)

# liste des comptes utilisateurs activés mais qui ne sont pas connectés depuis
# plus de 30 jours avec la date de leur dernière connexion
# et export du résultat vers le fichier ListeUser.csv
$ListeUser= Get-ADUser -Filter {LastLogonDate -lt $Limite -and enabled -eq $true} -Properties LastLogonDate | export-csv c:\ListeUsersInactifs.csv
```

Remarque : les parenthèses ne sont pas strictement nécessaires, mais peuvent être présentes, comme dans l'annexe.

```
$ListeUser= Get-ADUser -Filter {(LastLogonDate -lt $Limite) -and (enabled -eq $true)} -Properties LastLogonDate | export-csv c:\ListeUsersInactifs.csv
```

Mission B.2 – Dimensionnement d'une ferme de serveurs

Etude des serveurs de la ferme

Question B.2.1
Démontrer que les serveurs peuvent héberger, au minimum, les machines virtuelles demandées.

Côté vCPU
On demande, par serveur virtuel, 2 vCPU et 8 Go de mémoire vive.
Par serveur : 20 cœurs (2 processeurs), soit 40 vCPU avec l'Hyper-Threading, donc 20 MV
Avec les 3 serveurs : 120 vCPU. Donc la capacité de calcul permet d'héberger jusqu'à 60 MV requérant 2 vCPU.

Coté RAM

4 x 32 Go, soit 128 Go par serveur.
Avec les trois serveurs : 384 Go,

8 Go par VM ⇨ 48 VM maximum *(48 x 8 = 384 Go)*

Conclusion : Pour 20 VM, il faut 160 Go de RAM, ce qui est le cas puisque les trois serveurs permettent d'avoir 3 x 128 Go.

Il est bien possible d'héberger 20 serveurs virtuels. Car 60 VM possibles > 20 souhaitées et 48 > 20

Question B.2.2
Calculer combien de machines virtuelles au maximum pourraient héberger les serveurs, dans la configuration proposée. *Justifier votre réponse.*

Côté vCPU
Pour la ressource en puissance de calcul, donc de vCPU disponibles : la ferme de serveurs, dans sa configuration actuelle, peut héberger **60** serveurs virtuels

Côté RAM
Pour la ressource RAM, la ferme de serveurs peut héberger **48** serveurs virtuels.

La réponse est donc : **48** serveurs virtuels, ce qui correspond à la ressource la plus limitée.

Question B.2.3
Indiquer dans quelle mesure il est possible de faire évoluer la configuration des serveurs pour accueillir plus de machines virtuelles.
Vous préciserez quel est l'élément qui limite cette évolution.

La carte mère semble adaptée aux processeurs indiqués, dotés de 10 cœurs, donc à priori il n'est pas possible d'aller au-delà.

On peut ajouter de la mémoire vive. *(Jusqu'à 24 barrettes de 32 Go par serveur au lieu de 4 initialement, soit 768 Go par serveur), ce qui permettrait de sextupler la capacité mémoire, donc potentiellement le nombre de machines virtuelles, qui doivent être dotées de 8 Go de RAM :*

*Soit 48 x 6 = **288** MV (en repartant de la réponse à la question 2.2)*

ou 768 x 3 serveurs / 8 Go = 288 MV (la valeur exacte n'est pas exigée)

La réponse peut partir du maximum toléré par les 120 vCPU donc 60 MV, chaque MV a besoin de 8 Go donc 480 Go pour 3 serveurs, il faut donc 160 Go par serveur. Initialement, chaque serveur possède 128 Go, il faudra donc rajouter 32 Go (si possible en 2 fois 16 Go de manière à optimiser le dual-channel et le bi-CPU.

La ressource la plus contrainte devient alors le nombre de cœurs : le nombre de machines serait donc porté à 60 MV (au lieu de 48).

Remarque : il est possible d'envisager une surallocation au niveau vCPU (un facteur x2 est fréquemment utilisé en exploitation, voire plus pour des machines virtuelles de test).

La surallocation au niveau RAM est en revanche à éviter. En tous cas elle ne devrait pas dépasser un facteur de x1.5 d'après certains spécialistes.

Question B.2.4
Déterminer par le calcul si la baie de stockage, hors extension, peut héberger les 20 serveurs virtuels prévus.

On peut installer 16 disques de 2 To, soit 32 To.
Mais :
4 disques sont utilisés pour la gestion de l'ensemble.
Il reste donc 12 disques, à partager en deux systèmes RAID5.
Chaque système dispose d'un disque Hot spare.
On calcule donc la capacité d'un système EXPLOITATION RAID5 sur 5 disques de 2 To.
La capacité utile est de 4 x 2 = 8 To. On prévoit une capacité de 500 Go (marge de 200 Go) pour chaque serveur. On obtient donc la possibilité de dimensionner 16 disques virtuels, pour 16 machines virtuelles.

Il faut donc utiliser l'extension EMC SCv300, si l'on veut héberger plus de 16 machines virtuelles.

Il est rappelé qu'il faudra héberger plus de 20 machines virtuelles.
On décide d'utiliser l'extension EMC SCv300, et de tester la capacité pour 40 machines virtuelles.

Question B.2.5
Vérifier qu'avec l'extension, l'ensemble « RAID5 EXPLOITATION » permet d'héberger quarante machines virtuelles. *Vous préciserez le volume disponible supplémentaire éventuel.*

Avec l'extension, nous disposons de 12 disques supplémentaires, soit 6 par système RAID5 (6 pour EXPLOITATION, 6 pour REPLICATION).

Deux façons de procéder :

- *Refaire le calcul sur 28 disques (16 + 12), en comptant les 4 disques de gestion, les deux disques Hot spare, etc.*
- *Considérer que les disques de l'extension s'ajoutent directement aux ensembles déjà constitués.*

Chaque ensemble RAID5 compte 11 disques (28 - 4 de gestion - 2 de spare), pour une capacité utile de 20 To, permettant d'allouer un espace de stockage de 500 Go à 40 disques durs, donc pour 40 MV.

L'ensemble EXPLOITATION peut donc héberger 40 serveurs virtuels, mais pas plus.

D'après nos calculs précédents, la capacité de stockage devient donc la contrainte la plus forte, puisque la capacité de calcul et la mémoire (maximale) permettrait d'héberger respectivement 60 MV et 96 MV.

Haute disponibilité

Il est important que les serveurs virtuels soient toujours accessibles pour les entreprises clientes.

Question B.2.6
a) Justifier en quoi l'ensemble RAID5 avec disque de secours (*Hot spare*) contribue à l'exigence de haute disponibilité
b) Mentionner, parmi les autres spécifications techniques de la ferme de serveurs, au moins deux éléments qui contribuent également à cette exigence de haute disponibilité.

a)
Le RAID 5 se conçoit sur au minimum trois disques durs. Ce système est le système RAID le plus utilisé car il combine l'utilisation simultanée des disques, profitant donc de performances améliorées en lecture/écriture, et d'une tolérance aux pannes.
Ce système de parité permet de prévenir la panne d'un des disques durs présents. *La capacité totale de ce type de RAID est égale au total moins la capacité d'un disque (dû à la parité).*
Les données restent donc disponibles, mais la panne d'un disque n'entraîne aucune perte de données.

Le disque de secours permet une intégration immédiate de ce disque en remplacement et donc une reconstruction automatique de la grappe complète, ce qui limite le risque induit par une 2ème panne de disque, qui elle entraînerait une perte de données.

b)
Ce qui participe directement à la haute disponibilité :
Au niveau du local :
Alimentations sans interruption, branchées sur des circuits séparés.
Au niveau des serveurs :
2 blocs d'alimentation électrique redondants, échangeables à chaud.

Autres propositions possibles :
- Présence de 3 serveurs hôtes : il est probable que la version de VMWare permette de faire tourner les machines virtuelles sur les serveurs hôtes encore disponibles (fonctionnalité HA). Mais rien dans la documentation de le précise.
- Double contrôleur sur la baie (même si on ne précise pas exactement le mode de fonctionnement)
- Deux cartes réseau QLogic Quad port.
- La présence d'un Dual SD pour le système d'exploitation (même on n'indique pas précisément s'il s'agit d'une sauvegarde ou d'une réelle redondance)

Ce qui ne participe à priori pas à la haute disponibilité :

Climatisation du local : ne nuit pas au bon fonctionnement du matériel

Deux processeurs par serveur hôte : la documentation ne précise rien sur le fonctionnement redondant de ces processeurs.

Réplication entre les systèmes RAID5 EXPLOITATION et REPLICATION : la documentation ne précise pas si l'on passe d'un système disque à l'autre en cas de défaillance.