CAS MODEPRIVEE.SHOPPING

ÉLÉMENTS DE CORRIGÉ

Barème

Partie A	*Refonte de l'infrastructure*	45 points
Partie B	*Intégration dans l'équipe support*	35 points
Partie C	*Migration vers le cloud*	20 points
	Total	100 points

Dossier A – Refonte de l'infrastructure

Mission A.1 – Réorganisation des VLAN

Question A.1.1
Indiquer, en argumentant, en quoi le commutateur présélectionné permet de prendre en charge les mêmes fonctionnalités que les deux équipements à remplacer.

Les spécifications du commutateur proposé nous apprennent qu'il est **de niveau 3 puisqu'il permet le routage** (donc peut remplacer le routeur actuel) et propose également **la gestion des VLAN** (IEEE 802.1Q).

Les éléments sont repérables dans le Document 3 :

- Capacité : Routes IPv4
- Protocoles de routage : RIP-1, RIP-2, EIGRP
- Caractéristiques : Prise en charge du réseau local (LAN) virtuel
- Conformité aux normes : 802.1Q

Question A.1.2
Proposer, pour le nouveau VLAN destiné aux serveurs *Web*, un numéro de VLAN, une adresse de sous-réseau et un masque. *Justifier votre réponse.*

Le réseau principal est 172.29.64.0 /19. Il est découpé en 8 sous-réseaux en /22, donc les valeurs varient sur le 3ème octet :

64 **010**0 0000
68 **010**0 0100
72 **010**0 1000
76 **010**0 1100
80 **010**1 0000 (choix 1)

Nous pourrions avoir une solution cohérente sur les VLAN suivants comme :
84 ***010**1 0100* *(choix 2)*
88 ***010**1 1000* *(choix 3)*
~~***92*** ***0101 1100***~~ *Choix incorrect : Ce 4ème et dernier sous-réseau est déjà utilisé pour le sous-réseau entre FW-1 et RT-1.*

Le prochain sous-réseau disponible est donc 172.29.**80**.0 255.255.252.0 (Choix 1)
Mais on acceptera les 2 autres sous-réseaux disponibles.

*Pour respecter la demande (même nombre d'hôtes) le masque doit être **255.255.252.0**.*
Si on veut garder la cohérence avec le plan d'adressage, le n° de VLAN est identique à la valeur du 3ème octet du sous-réseau concerné.

Question A.1.3
Indiquer si la configuration IP des serveurs SRV-IIS-1 et SRV-IIS-2 doit être modifiée suite à l'implantation de ce nouveau VLAN et proposer les paramètres, en conformité avec l'existant, des autres VLAN si nécessaire.

Les serveurs vont changer de VLAN donc il faudra leur attribuer une nouvelle adresse IP, un masque de sous-réseau et une passerelle par défaut dans le nouveau VLAN.

Pour garder une cohérence avec les passerelles existantes (pour les 4 autres VLAN). Il faut donc affecter à la nouvelle passerelle la dernière adresse IP affectable sur son sous-réseau IP (c'est le cas sur les 4 VLAN existants).

En gras la réponse attendue ; au-dessous les autres réponses acceptées

Choix	*1ère adresse IP possible*	*Dernière adr. IP possible*	*Exemple Adresse IP*	*Masque*	*Passerelle*
Choix 1	**172.29.80.1**	**172.29.83.253**	**172.29.80.201**	**255.255.252.0**	**172.29.83.254**
Choix 2	172.29.84.1	172.29.87.253	172.29.84.201	255.255.252.0	172.29.87.254
Choix 3	172.29.88.1	172.29.91.253	172.29.88.201	255.255.252.0	172.29.91.254

La demande de cohérence pourrait également s'appliquer à l'affectation des adresses IP des serveurs mais nous accepterons toute solution cohérente pour le nouvel adressage IP de ces serveurs.

Suite à la virgule située après « existant », le candidat pourrait comprendre que la question porte dans un deuxième temps sur des modifications liées uniquement aux autres vlan. Dans ce cas, le candidat pourrait indiquer qu'aucun changement n'est nécessaire, ce qui serait une réponse correcte.

Question A.1.4
Expliquer pourquoi les tests ont échoué et proposer une solution pour remédier à ce problème.

On remarque dans le document A3 que le ping entre le serveur SRV-SQL-1 et sa passerelle 172.29.75.254 réussit.
Par contre ce serveur ne ping pas le serveur SRV-IIS-1.

Les deux autres tests permettent d'affiner le diagnostic pour comprendre pourquoi la communication entre SRV-SQL-1 et SRV-IIS-1 n'est pas possible :

- SRV-IIS-1 a une passerelle bien configurée, mais ne peut pas pinguer sa passerelle, donc la communication ne fonctionne pas avec le commutateur SW3-1 qui joue le rôle de passerelle.
- La réussite du test complémentaire depuis SRV-SQL-1 sur la passerelle associée au nouveau VLAN prouve que le routage est activé sur SW3-1 et que l'interface SVI (Switch Virtual Interface ou interface virtuelle du commutateur) est correctement configurée sur SW3-1.

En observant la configuration du SW3-1, on constate qu'il manque une autorisation dans le trunk vers le nouveau VLAN 80 *(ou tout autre VLAN choisi)* :

Configuration actuelle (incomplète)
switchport trunk allowed vlan 64, 68,72, 76

Configuration corrigée
switchport trunk allowed vlan 64, 68,72, 76**, 80**.

Possibilité de commande d'ajout, par exemple : switchport trunk allowed vlan add **80**
Les commandes peuvent être abrégées, la réponse du candidat peut stipuler l'ajout du vlan 80 sans forcément réécrire la ligne mais il doit faire une allusion à cette dernière

Cette configuration est nécessaire et devrait résoudre le problème

Mission A.2 –Mise en production d'un élément actif

Question A.2.1
a. Argumenter sur le choix d'un protocole sécurisé d'accès à distance compatible avec le nouveau commutateur.
b. Lister les points à vérifier lors de la configuration de ce protocole afin d'obtenir le meilleur niveau de sécurité*. Justifiez votre réponse.*

a. Le protocole SSH (voir caractéristiques / document 3) permet d'administrer l'appareil au travers du réseau via un **canal de communication chiffré** (un tunnel). Celui-ci **rend les données échangées illisibles en cas de capture de la communication**. *C'est d'autant plus important qu'un mot de passe d'administration sera utilisé pour intervenir sur l'appareil.*
Les autres protocoles listés dans le document 3 ne répondent pas à cette exigence.

b. Plusieurs points de vérification peuvent être avancés

- Une clé de cryptage de longueur suffisante pour éviter qu'elle soit « cassée ». *2048 pourrait être un minimum.*
- L'utilisation de la version 2 est à plébisciter car son algorithme est plus robuste face à certaines attaques que ceux de la version 1.
- La désactivation du protocole Telnet (sur toutes les interfaces d'administration) : Il faut donc absolument le désactiver pour imposer une administration à distance uniquement via SSH. Sans désactivation il sera toujours possible d'établir une connexion non sécurisée.
- Désactiver d'autres protocoles non sécurisés éventuels comme HTTP (pour accéder au site web d'administration embarqué sur le commutateur).
- Un filtrage par une règle de pare-feu, permettant par exemple uniquement les flux SSH à destination de cet équipement.
- L'authentification renforcée (mot de passe fort ou certificat côté client).

Question A.2.2
a) Argumenter sur l'importance de centraliser les journaux des événements système sur un serveur et de synchroniser les horloges entre tous les appareils.
b) Vérifier si le commutateur retenu peut répondre à ces deux besoins.

a)
La surveillance des journaux système est une des tâches de base de l'administrateur-trice.
Une analyse régulière, éventuellement assistée par des outils qui automatisent la mise en évidence des informations importantes ou anormales, est une bonne pratique qui peut permettre de révéler des anomalies en amont. **La consultation des journaux en un seul point facilite les contrôles réguliers et l'analyse en cas d'alerte**. De plus la panne d'un équipement pourra permettre la consultation des derniers événements remontés sur le serveur de centralisation.

Le serveur syslog recueillera des journaux provenant de différentes machines, ceux-ci sont systématiquement horodatés. **La synchronisation parfaite des horloges des appareils facilitera la reconstitution des événements** par exemple si plusieurs appareils ont été compromis.

b)
Le protocole standard pour transférer les journaux (*logs*) entre un appareil et un serveur est ***syslog*.** Le **commutateur supporte ce protocole** (voir caractéristiques / document 3 : « prise en charge de Syslog »).

Le protocole internet pour synchroniser les horloges est **NTP (*Network Time Protocol*) qui est bien supporté par le commutateur** (toujours dans les caractéristiques / document 3 : « prise en charge de NTP (Network Time Protocol) »).

Question A.2.3
Lister les principaux paramétrages à réaliser lors de la configuration de l'agent SNMP sur le commutateur.
Pour chaque paramétrage, vous argumenterez en termes de risques potentiels et de sécurisation.

SNMP est un protocole relativement « bavard » qui, s'il est mal configuré, peut révéler des informations sensibles sur un appareil. Il permet également de modifier à distance certains paramètres.

A minima, la configuration d'un agent SNMP nécessite de mettre un nom de communauté (qui agit comme un « mot de passe ») entre la plateforme de supervision et l'appareil. **On bannira l'usage du nom de communauté par défaut « public »** et on choisira un nom différent, plus long, intégrant un jeu de caractères varié. On configurera l'accès en « lecture seule » pour éviter la modification.

Dans les autres bonnes pratiques, on peut citer :
- n'autoriser que l'IP de la plateforme de supervision à interroger l'appareil,
- limiter les OID interrogeables au strict nécessaire
- activer la version 3 de SNMP - si les équipements concernés le supportent – ce qui permet de chiffrer les échanges (ce qui est le cas sur ce commutateur).

Question A.2.4
Proposer deux commandes de vérification pertinentes pour la supervision du nouveau commutateur, en précisant les valeurs des paramètres. *Justifiez votre réponse.*

Les commandes de vérification pertinentes pour la supervision du nouveau commutateur pourraient être :

check_centreon_ping (ARG1 : nombre de ping incorrects avant une alerte) pour vérifier la disponibilité de l'appareil. Par exemple ARG1=3 pour 3 pings (3 pts)

check_centreon_traffic (ARG1 : on mettra les interfaces du switch G1/0/1, G1/0/2, etc., ARG2 : seuil de trafic pour un avertissement 70 % par exemple, ARG3 : seuil de trafic pour une alerte critique 90 % par exemple) pour surveiller la charge réseau interface par interface. (3 pts)

D'autres commandes peuvent être pertinentes mais il faut que la proposition du candidat ou de la candidate soit accompagnée d'une explication cohérente avec le besoin de vérification.
D'autres ne peuvent pas l'être (ex : check_centreon_nt, check_centreon_remote_storage, etc…)

Dossier B – Intégration dans l'équipe support

Mission B.1 – Saturation d'un lien sur le commutateur

Question B.1.1
Proposer une solution permettant d'augmenter le débit en vous appuyant sur les spécifications des cartes réseau des serveurs ESX et du commutateur.

Pour améliorer le débit, on peut envisager **d'agréger des ports réseau entre le commutateur et les serveurs afin de multiplier le débit** entre ces appareils.
Il faut vérifier que côté serveur et **côté commutateur un protocole d'agrégation de port est supporté**. Dans les spécifications du commutateur, on observe que celui-ci supporte l'agrégation de ports via les protocoles **LACP et PagP**. De plus, il dispose de 24 ports mais seuls 6 ports sont actuellement utilisés. **Côté serveur**, on constate également la **disponibilité du protocole LACP (802.3ad)**. L'agrégation de port est donc possible. (4 pts)

A noter que VMWare peut gérer nativement (via un vSwitch gérant plusieurs interfaces du serveur) la répartition de charges sur plusieurs cartes physiques, sans configuration spécial du commutateur.

Mission B.2 – Activité suspecte sur un serveur web

Question B.2.1
Sur la base de l'extrait de journal fourni, argumenter pour confirmer qu'il s'agit bien d'une activité suspecte.

*On constate que l'adresse IP de l'émetteur est **toujours la même** (180.222.224.52)* et que les **requêtes HTTP sont reçues dans un intervalle très bref**. De plus, les URL demandées sont aléatoires et gérés par des navigateurs clients supposés différents
Il s'agit vraisemblablement d'une attaque par déni de service (DOS) qui cherche à saturer le serveur victime.

Question B.2.2
a. À court terme, indiquer sur quel appareil de l'infrastructure intervenir et quel type de configuration réaliser pour bloquer cette activité suspecte.
b. À plus long terme, proposer une solution matérielle et/ou logicielle pour automatiser la détection et le blocage de ce type d'activité.

a. A court terme, on pourrait configurer une règle qui bloque l'IP de l'attaquant, de préférence sur le pare-feu FW-1 en tête de réseau ou à défaut sur le serveur web lui-même via un pare-feu installé localement (iptables sous Linux ou pare-feu « personnel » sous Windows).

b. A plus long terme, on peut proposer de mettre en place une solution IPS (Intrusion Prevention System ou système de prévention aux intrusions) *ou solution équivalente de blocage pour ce type d'activité.*
Une solution basée sur un système de détection d'intrusion (IDS) pourra être envisagée mais ne pourra pas répondre entièrement au besoin, plus particulièrement celui de blocage.

Mission B.3 – Traitement d'un courriel d'alerte

Question B.3.1
a. À la lecture du courriel, identifier le ou les composants concernés.
b. Proposer une catégorie pour cet événement.
c. Proposer en argumentant une priorité selon la matrice de priorisation des incidents.

a. CI fait partie du vocabulaire ITIL et désigne un élément de configuration stocké dans la CMDB. Ici, l'entête du courriel indique qu'il s'agit du serveur SRV-SQL-1 *et plus précisément de la carte contrôleur RAID.*

b. Le document 6 nous permet d'établir la catégorie : Matériel > Serveur > Disque (un disque physique de la grappe RAID est en échec (FAILED))

c. Dans l'immédiat, **l'impact est « faible »** puisque cette grappe RAID est configurée en mode RAID 0+1 et donc permet une tolérance aux pannes puisqu'il s'agit de miroir. Concernant l'urgence, ce n'est pas une urgence absolue puisqu'il n'y a pas d'interruption de service, néanmoins la situation ne peut rester en l'état et un remplacement du disque est à prévoir rapidement. Selon l'argumentation, on acceptera une **urgence « moyenne » ou « haute ».**
(D'autant que la perte d'un disque sur l'autre grappe serait fatale)
La **priorité** est donc moyenne, **entre 3 et 4**.

Question B.3.2
a. Indiquer les informations que vous avez besoin de rechercher dans la base de données de gestion de configuration pour préparer l'intervention.
b. Rédiger un courriel à destination de l'administrateur système dans lequel sera indiqué votre diagnostic ainsi que les conséquences et risques prévisibles.

a. La base de données de configuration, issue d'un inventaire automatique du parc, doit nous fournir toutes les informations nécessaires à l'intervention. Pour le disque concerné, nous devons connaître : **type d'interface (SAS ou SATA), type de disque (HDD ou SSD), capacité.** De plus, on doit avoir **des informations sur une éventuelle garantie ou contrat de maintenance** afin de déterminer les responsabilités, et contacter le fournisseur concerné le cas échéant.

b.
De : support@modeprivee.shopping
A : admin-systeme@modeprivee.shopping
Sujet : Problème système disque

Bonjour,

Suite à une alerte envoyée par la plateforme de supervision, signalant un problème sur le système RAID (0+1), je peux vous communiquer les informations suivantes

- Un disque de 800 GB est déclaré défaillant sur la 1ère grappe du miroir
- Cet incident n'est pas bloquant puisque tous les disques de la 2ème grappe sont déclarés OK ; il n'y a donc pas d'interruption de service.
- La 1ère grappe est donc globalement en défaut. En cas de défaillance d'un disque sur la 2ème grappe, on pourrait avoir une conséquence fâcheuse, puisque les données ne seraient plus accessibles. Il convient donc de remplacer le disque défectueux dans les meilleurs délais.

Cordialement,
MOI

*Les éléments à indiquer dans le courriel sont donc : **diagnostic** (un disque SSD en panne sur une grappe RAID dans le premier miroir), **conséquence** (pas d'interruption de service), **risques prévisibles** (disque à remplacer dès que possible car sinon la tolérance aux pannes peut être compromise en cas de panne d'un autre disque).*

Question B.3.3
a) Justifier la qualification de cet incident en problème, au sens du référentiel ITIL.
b) Lister les recherches à réaliser et les étapes nécessaires pour régler de manière permanente ce problème.

a)
Un incident est un événement ponctuel qui doit trouver une solution rapidement (remplacer le disque défectueux). Mais si celui-ci **se reproduit**, nous sommes alors en présence d'un problème. Dans ce cas, il faudra rechercher les causes et trouver une solution de plus long terme. Donc, il faut rechercher dans la base des tickets, pour le « *CI* » concerné, si un problème similaire s'est déjà produit.
Ici nous sommes en face d'un problème puisqu'il y a récurrence : 4 pannes de disque en 6 mois sur le même équipement révèlent une anomalie.

b)
Il faut aller sur le site internet du constructeur du serveur. A partir du numéro de série de l'appareil, il sera possible de consulter une base de connaissances. Si c'est un problème connu (mauvaise série par exemple), une solution sera proposée. Sinon, il faudra faire une recherche et vérifier les versions de micrologiciel (*firmware*) de la carte contrôleur et des disques afin de s'assurer que tout est à jour.

On peut imaginer d'autres causes : problèmes d'alimentation, incompatibilité des disques, possibilité d'erreur humaine, défaut sur la baie

Dossier C – Migration vers le *cloud*

Mission C.1 – estimation du coût de la migration

Question C.1.1
Expliquer pourquoi certains coûts ne sont pas facturés par le Centre de données à ModePrivee.Shopping pour la location de l'armoire technique.

Sur la base du document 1, les coûts qui peuvent être facturés au client sont :

- Un loyer de la baie (ou de l'emplacement)
- La consommation électrique
- Les cross-connects
- Le hands and eyes

Les deux derniers points ne sont pas pertinents :

- Il n'y a pas de cross-connects, puisqu'il n'y a pas de liaison spéciale à prévoir avec une autre armoire, ni sur le site, ni sur un autre site.
- Le datacenter est proche de la DSI, donc ces coûts sont nuls, puisque les gestes de proximités seront réalisés par des employés de ModePrivee.Shopping.

Question C.1.2
Calculer le coût de revient total de l'armoire technique sur 5 ans, prenant en compte les éléments facturés par le propriétaire du centre de données et le matériel (renouvelé tous les 5 ans).

SOLUTON ARMOIRE LOUEE		
SERVEURS	15 000,00 €	
BAIE DE STOCKAGE	5 000,00 €	
COMMUTATEUR	3 000,00 €	
PAREFEU	2 000,00 €	
LOYER ARMOIRE TECHNIQUE	150 000,00 €	12 mois x 2 500 x 5 ans
CONSOMMATION ELECTRIQUE	5 000,00 €	1 000 Euros par an
TOTAL POUR 5 ANS	180 000,00 €	

Le coût total estimé pour 5 ans est de 180 000,00 Euros
A noter qu'il ne tient pas compte de la main d'œuvre pour les interventions des salariés de ModePrivee.Shopping.

Question C.1.3
Calculer le coût d'hébergement sur 5 ans des machines virtuelles dans le *cloud*, sachant qu'en plus des serveurs *Web* et des serveurs de base de données, un serveur d'authentification sera nécessaire.

SOLUTION *CLOUD*

VM SQL SERVER x 2	120 000,00 €	12 000 x 5 ans x 2 VM
VM IIS x 2	50 000,00 €	5 000 x 5 ans x 2 VM
CD x 1	5 000,00 €	1 000 x 5 ans
TOTAL POUR 5 ANS	175 000,00 €	

Le coût total estimé pour 5 ans est de 175 000,00 Euros
A noter qu'il comprend toute intervention éventuelle sur les serveurs pour des problèmes matériels

Question C.1.4
Identifier les avantages et inconvénients de cette nouvelle solution :
a. d'un point de vue économique (financier)
b. en termes d'administration des serveurs
c. en termes de fonctionnement (disponibilité des ressources, performances, etc.)
d. en termes d'évolutivité de l'infrastructure

	Avantages	Inconvénients
Point de vue économique	Les coûts théoriques peuvent sembler similaires Mais il n'y aura pas de coûts cachés liés à la maintenance des serveurs physiques et autres équipements de la baie ou au renouvellement de ceux-ci *En théorie il y aura une économie de main d'œuvre, celle qui était nécessaire pour les interventions dans le datacenter, le renouvellement des machines, etc …* Les frais sont forfaitaires donc prévisibles d'un point de vue financier.	On n'a pas de certitude sur l'évolution des prix du *cloud* et surtout les prix risquent d'être beaucoup plus élevés si le trafic et les ressources provisionnées ont été sous-estimés. On peut regretter de ne pas pouvoir installer d'autres machines virtuelles sans payer de surcoût, ce qui n'était pas le cas dans la solution de location d'emplacement.
Administration des serveurs	Absence de maintenance matérielle Les ressources humaines en interne pourront se recentrer sur le développement et l'assistance aux utilisateurs	Dépendante de la connexion au *cloud*. Des interventions imprévues pourront être facturées car hors forfait (exemples : reboot, branchement de jarretière, …)
Disponibilité, ressources, performances	Normalement, le fournisseur garantit une haute disponibilité, des performances à la demande…	Performances et disponibilité augmentent le prix Perte de maîtrise de la localisation et la traçabilité des données. (allusion possible au RGPD)
Évolutivité	Pas d'investissement matériel Evolutivité rapide Evolutivité ponctuelle pour un pic d'activité	Le prix augmente en proportion, et on n'a pas forcément de visibilité sur la tarification.

Mission C.2 – migration d'un serveur web dans le *cloud*

Question C.2.1
Indiquer la solution que vous retenez en argumentant par rapport à la principale contrainte de mise à disposition rapide du site *Web* sur la nouvelle machine virtuelle.

La modification de la zone DNS implique un temps de propagation de la nouvelle configuration qui peut être assez long (vers les serveurs secondaires, les serveurs de cache, les caches locaux …). On peut également ne pas avoir la possibilité d'intervenir directement sur les fichiers de zone.

Le plus simple et le plus rapide, à court terme, est de configurer une redirection HTTP sur le serveur Web. Cela sera transparent pour les testeurs.

En revanche cette solution n'est pas souhaitable comme solution pérenne.

La redirection HTTP ne concernera pas le service FTP (si actif)