Questionnaire professionnel

**1. Assurer le support utilisateur en centre de service (CCP 1)**

1.1

Selon ITIL (Information Technology Infrastructure Library) :

* Incident : C'est un événement imprévu qui perturbe ou diminue la qualité d'un service informatique. L'objectif avec un incident est de rétablir le service le plus rapidement possible.
* Problème : C'est la cause sous-jacente ou inconnue d' un ou plusieurs incidents. L'objectif de la gestion des problèmes est d'identifier et de résoudre ces causes, de manière à prévenir la récurrence des incidents associés.

1.2

Les différents moyens de prendre le contrôle à distance d’une machine sont :

* Le bureau à distance Windows : qui utilise Remote Desktop Protocol (RDP)
* Les logiciels dédiés : comme VNC, TeamViewer, AnyDesk, ou Microsoft SCCM
* Les commandes à utiliser dans un terminal : comme le Remote PowerShell, ou les connexions SSH (principalement pour les systèmes basés sur Unix/Linux), à noter que l’on peut utiliser SSH avec X11 pour un retour graphique
* Les outils basés sur le web : Comme Chrome Remote Desktop.
* Également les connexions VPN : en établissant un tunnel VPN, on peut accéder au réseau distant et ensuite utiliser des outils locaux pour se connecter aux machines.

1.3

Dans une résolution d’incident par téléphone, voici les différentes étapes à respecter :

* Identification / Détection
* Notification
* Enregistrement
* Catégorisation et priorisation
* Diagnostic et investigation
* Suivi (ou escalade)
* Résolution (et documentation)
* Clôture

**2. Exploiter des serveurs Windows et un domaine Active Directory (CCP 2)**

2.1

Un rôle FSMO (Flexible Single Master Operation) est la possibilité pour un contrôleur de domaine, sur un domaine Active Directory, de pouvoir effectuer des tâches particulières.

Il existe 5 rôles FSMO :

* Maître de schéma
* Maître d’attribution de nom de domaine
* Maître RID
* Maître d’infrastructure
* Émulateur PDC

2.2

La réplication entre contrôleurs de domaine est primordiale pour les raisons suivantes :

* Elle garantie la cohérence et la disponibilité des données d'annuaire dans un environnement réseau
* Elle permet de s'assurer que toutes les modifications (comme les ajouts d'utilisateurs, les modifications de mots de passe, et les politiques de groupe) sont uniformément réparties à travers tous les contrôleurs de domaine, assurant ainsi que les utilisateurs ont accès aux informations les plus à jour, peu importe à quel contrôleur de domaine ils se connectent
* Elle amène de la tolérance de panne.

**3. Exploiter des serveurs Linux (CCP 3)**

3.1

Cette commande ajoute le droit d'exécution « +x » au propriétaire « u » pour le fichier « /home/tssr/factures/exports.sh ».

3.2

La commande est :

ip address add 172.16.8.16/24 dev enp0s8

Ensuite il faudra activer l’interface avec “ip link set dev enp0s8 up”

3.3

Cause probable : l’utilisateur "wilder" n'a pas les permissions nécessaires pour accéder au dossier.

Pour vérifier les permissions : ls -ld /home/wilder/travaux/

Pour résoudre le problème on peut :

* Changer les permissions avec (par exemple) “chmod 750 /home/wilder/travaux”
* Modifier le propriétaire avec (par exemple) “chown wilder:wilder /home/wilder/travaux/”

3.4

Le périphérique actuel est /dev/sda1, donc si on ajoute un disque dur avec une seule partition, elle se nommera sdb1.

3.5

On peut utiliser « lsblk » et « fdisk –l ».

**4. Exploiter un réseau IP (CCP 4)**

4.1 Complète le tableau ci-dessous :

| **Adresse de réseau** | **CIDR** | **1ere adresse disponible** | **Dernière adresse disponible** | **Adresse de broadcast** |
| --- | --- | --- | --- | --- |
| 192.160.16.0 | 255.255.255.224 | 192.160.16.1 | 192.160.16.30 | 192.160.16.31 |
| 192.160.16.32 | 255.255.255.224 | 192.160.16.33 | 192.160.16.62 | 192.160.16.63 |

4.2 Complète le tableau ci-dessous :

| **Décimal** | **Binaire** | **Hexadécimal** |
| --- | --- | --- |
| 9 | 0000 1001 | 0x 09 |
| 127 | 0111 1111 | 0x 7F |
| 255 | 1111 1111 | 0x FF |
| 16 | 0001 0000 | 0x 10 |

4.3

Liens trunk ?

Ce sont les liens entre les switchs et le lien entre un switch et le routeur.

Méthode de routage ?

Le routeur se charge de router entre les VLANs avec des id de vlans différents sur le même medium. La méthode de routage est « Router-on-a-stick ».

4.4

Solution matérielle :

Installer un routeur pour interconnecter les deux sous-réseaux.

Chaque PC sera connecté à une interface du routeur, et le routeur assurera la communication entre les deux sous-réseaux.

Modification du paramétrage :

Bien vérifier que PC1 utilise l’interface du routeur sur laquelle il est connecté comme passerelle par défaut. Même chose pour PC2 pour l’autre interface.

4.5

Pour PC1 ?

Il a l’adresse de réseau 192.168.10.0/24 qui est la même que celles de PC2 donc le ping fonctionne avec cette machine.

Cette adresse de réseau est également un sous-réseau de celle de PC3, donc il peut renvoyer une trame « echo reply» à une demande « echo request » de PC3.

Il ne peut pas communiquer directement avec PC4 car ils sont dans des réseaux différents.

Pour PC2 ?

Son adresse de réseau est 192.168.10.0/24, donc il peut communiquer avec PC1. Comme PC2, cette adresse est dans un sous-réseaux de l’adresse réseau de PC3, donc il peut également envoyer une trame « echo reply» à une demande « echo request ».

Pour PC3 ?

Il a l’adresse de réseau 192.168.0.0/16. Pour un ping vers PC1, PC3 prend l’adresse IP destination avec son propre masque, ce qui donne l’adresse de réseau « fictive » 192.168.0.0/16 pour PC1. PC3 considère alors que PC1 est dans son réseau et peut envoyer une trame « echo request ». PC1 peut répondre à cette requête.

Même chose pour PC2.

Pour PC4, PC3 « considère » qu’il a l’adresse de réseau 192.168.0.0/16 et donc lui envoie une trame « echo request ».

Pour PC4 ?

Son adresse de réseau est 192.168.11.0/24. Elle est différente de celle de PC1. Les 2 machines ne peuvent pas communiquer.

Même constat avec PC2.

Pour PC3, PC4 considère que son adresse de réseau est 192.168.10.24, donc ils ne sont pas dans le même réseau et PC4 ne peut pas envoyer une trame de réponse à la demande « echo request » de PC3.

En conclusion, seul les PC1, PC2, et PC3 peuvent communiquer entre-eux.

4.6

Les actions possibles sont :

* Changer le nom du SSID : Modifiez le nom par défaut du réseau
* Désactiver la diffusion du SSID (le cacher)
* Durcir le chiffrement (par exemple WPA2 Entreprise ou WPA3)
* Changer le mot de passe par défaut : Choisir un mot de passe fort et unique
* Utilisez un réseau invité pour les personnes extérieures à l’entreprise
* Mettre à jour le firmware des bornes wifi

4.7 Compléter le tableau ci-dessous (ajouter des lignes si besoin) :

| **Adresse de réseau** | **CIDR** | **Adresse de passerelle** | **Interface locale** |
| --- | --- | --- | --- |
| 192.168.1.0 | 255.255.255.0 | 172.14.1.1 | 172.14.1.2 |
| 192.168.2.0 | 255.255.255.0 | 41.11.21.1 | 41.11.21.2 |

4.8 Compléter le tableau ci-dessous :

| **Acronyme** | **Nom complet** | **Port(s) par défaut TCP** | **Port(s) par défaut UDP** |
| --- | --- | --- | --- |
| HTTP | Hypertext Transfer Protocol | 80 |  |
| FTP/FTPS | File Transfer Protocol / File Transfer Protocol Secure | 20 (données), 21 (commandes) |  |
| SSH | Secure Shell | 22 |  |
| TFTP | Trivial File Transfer Protocol |  | 69 |
| SMTP | Simple Mail Transfer Protocol | 25 (non-sécurisé), 587, 465 (sécurisé) |  |
| IMAP | Internet Message Access Protocol | 143 (non sécurisé), 993 (sécurisé) |  |
| LDAP | Lightweight Directory Access Protocol | 389 (non sécurisé), 636 (sécurisé) |  |
| POP3 | Post Office Protocol version 3 | 110 (non sécurisé), 995 (sécurisé) |  |
| DNS | Domain Name System | 53 | 53 |
| NTP | Network Time Protocol |  | 123 |
| POP3S | Post Office Protocol version 3 sécurisé | 995 |  |

4.9

Le téléphone IP a un chargeur donc on peut le brancher sur tous les ports, donc de 1 à 8.

4.10 Compléter le tableau ci-dessous :

| **Protocole** | **Accès réseau** | **Internet** | **Transport** | **Application** |
| --- | --- | --- | --- | --- |
| ARP | x | x |  |  |
| Ethernet | x |  |  |  |
| ICMP |  | x |  |  |
| IPv6 |  | x |  |  |
| DHCP |  |  |  | x |
| FTP |  |  |  | x |
| TLS/SSL |  |  | x | x |
| POP3 |  |  |  | x |
| Telnet |  |  |  | x |
| SNMP |  |  |  | x |

**5. Maintenir des serveurs dans une infrastructure virtualisée (CCP 5)**

5.1

Définition :

Un cluster d'hyperviseurs est un regroupement de plusieurs serveurs (ou nœuds) sur lesquels sont installés des hyperviseurs, permettant de gérer des machines virtuelles (VM).

Intérêt :

L’intérêt est de pouvoir répartir les VM sur plusieurs nœuds pour avoir de la haute disponibilité, une répartition de charge, et une gestion centralisée des ressources. Des protocoles comme le ceph peuvent être mis en place pour cela.

On a ainsi une continuité de service même en cas de défaillance d'un serveur.

5.2

Définition :

Un conteneur est une unité standardisée qui permet d’encapsuler, d’isoler, du code et toutes ses dépendances. L’application ainsi contenue s’exécute de manière fiable quel que soit l’environnement ou l’OS.

Exemples de solutions :

Docker,LXC

5.3

Signification :

Ces lignes de code sont le contenu d’un fichier Dockerfile. Il permet de construire une image Docker.

Voici les actions faites :

* Il part de l'image Ubuntu
* Installe les paquets bash et nano
* Supprime les sources téléchargées
* Crée un répertoire « /data » et définit ce répertoire comme répertoire de travail
* Lance une session Bash interactive lorsque le conteneur est démarré

Utilisation :

Pour exécuter ce code, on le sauvegarde dans un fichier nommé « Dockerfile », puis on construit l'image avec la commande « docker build ».

5.4

On voit une erreur « CRITICAL » sur le service « Swap usage ». On voit « 0% free » dans la colonne « Status informations ».

Il faut donc augmenter la taille du swap.

5.5

PaaS :

PaaS (Platform as a Service) : Fournit une plateforme pour développer et gérer des applications sans se soucier de l'infrastructure nécessaire.

IaaS :

IaaS (Infrastructure as a Service) : Offre des ressources informatiques virtualisées sur Internet, éliminant le besoin d'acheter ou de gérer une infrastructure physique.

SaaS :

SaaS (Software as a Service) : Logiciels hébergés dans le cloud auxquels les utilisateurs accèdent et utilisent via Internet, souvent via un navigateur web.

5.6

Les éléments indispensables sont :

* La redondance matérielle (serveur, stockage)
* Un système de répartition de charge (Load Balancing)
* Un système de basculement automatique en cas d’erreur ou de panne (Failover)
* Une copie (réplication) des données en temps réel
* Un système de supervision
* Un PRA et PCA

**6. Maintenir et sécuriser les accès à internet et les interconnexions des réseaux (CCP 7)**

6.1

Impact pour la machine :

Pour l’ACL 100 :

* Elle bloque le trafic ICMP (donc le ping) de 172.16.0.10 vers le réseau 172.17.0.0/24
* Elle autorise tout le reste du flux réseau

Pour l’ACL 101 :

* Elle bloque tout le trafic HTTP et HTTPS (donc le web) de 172.16.0.10 vers la machine 220.0.0.60
* Elle autorise tout le reste du flux réseau

Fusion des ACL :

access-list 110 deny icmp host 172.16.0.10 172.17.0.0 0.255.255.255

access-list 110 deny tcp host 172.16.0.10 host 220.0.0.60 eq www

access-list 110 deny tcp host 172.16.0.10 host 220.0.0.60 eq 443

access-list 110 permit ip any any

6.2

La commande passé derrière le « pipe » est « sha512sum » qui est une fonction de hachage cryptographiques.

Ce type de fonction de chiffrement produit toujours une sortie de taille fixe, quelle que soit la taille de l'entrée. C'est une caractéristique essentielle qui garantit que la sortie (le hachage) a une longueur constante.

6.3

Il faut :

* Créer sur le firewall une redirection des ports 80 (HTTP) et 443 (HTTPS) vers l’adresse IP du serveur web qui est dans la DMZ
* Créer une règle pour autoriser le trafic du WAN (Internet) vers l’adresse IP du serveur web qui est dans la DMZ sur les ports 80 et 443

6.4

VPN A :

VPN type accès distant (host to network)

VPN B :

VPN type site à site

6.5

Expression 1 :

La clé publique

Expression 2 :

Sa clé privée

Expression 3 :

asymétrique

6.6

Texte traduit :

Lorsque les négociations ISAKMP commencent, le nœud qui initie la négociation envoie toutes ses politiques au nœud distant, et le nœud distant essaie de trouver une correspondance.

Le nœud distant vérifie toutes les politiques du nœud initiateur contre chacune de ses politiques configurées dans un ordre de priorité (la plus haute priorité en premier) jusqu'à ce qu'il trouve une correspondance.

6.7

Menace 1 :

Les attaque par déni de service (DDoS)

Menace 2 :

Les ransomware

Menace 3 :

Les attaque virales

**7. Mettre en place, assurer et tester les sauvegardes et les restaurations des éléments de l’infrastructure (CCP 8)**

7.1

La règle du 3-2-1 est une pratique courante :

* 3 copies (prod + 2 sauvegardes)
* 2 types de support différents
* 1 copie hors-site

7.2

Les différents types de sauvegarde sont :

* Les sauvegarde complète
* Les sauvegarde incrémentale
* Les sauvegarde différentielle

7.3

Une sauvegarde est une copie de données en production actuellement utilisées. On peut les restaurer en cas de perte ou de corruption.

L’archivage est un stockage à long terme de données qui ne serve plus à la production, mais qui doivent être conservées pour des raisons légales ou historiques. Les données sont supprimées de la production.

Le clonage est la réplique exacte d'un système ou d'un disque dur, souvent utilisé pour déployer des configurations identiques sur plusieurs machines.

**8. Exploiter et maintenir les services de déploiement des postes de travail (CCP 9)**

8.1

Avantages :

Gestion simplifié et centralisée, politique de sécurité unifiée, réduction des coût de maintenance.

Exemple de solution :

WSUS (Windows Server Update Services) est un rôle sur un serveur Windows qui permet de gérer, de télécharger, et de publier des mises à jour à des postes clients au sein d’un parc informatique.

8.2

Les inconvénient sont les suivants :

* Dépendance au réseau
* Point de défaillance unique (serveur central par exemple)
* Coût initial (infrastructure de serveur pour les clients légers)
* Personnalisation limitée (au niveau utilisateur)

8.3

Signification :

La commande sysprep s’exécute dans cet exemple avec les commandes suivantes :

* /oobe : démarre la machine avec des fenêtres pour guider l’utilisateur
* /generalize : supprime les informations spécifiques au système, ce qui permet de réutiliser cette image sur d'autres machines (Id, ...)
* /shutdown : éteint la machine après que sysprep soit finalisé

Contexte d’utilisation :

Cette commande s’utilise pour préparer une image Windows en tant que « master » pour un déploiement de masse.

8.4

Il permet :

* Une accélération des mises à jour sur les clients
* La même version des paquets sur l’ensemble du parc informatique
* Une amélioration de la sécurité car un contrôle est fait par les membres de l’IT sur les paquets