Activité 1 : Exploiter les éléments de l’infrastructure et assurer le support aux utilisateurs

4 compétences types :

* Assurer le support utilisateur en centre de services
* Exploiter des serveurs Windows et un domaine Active Directory
* Exploiter des serveurs Linux
* Exploiter un réseau IP

Durée : 2h

**CCP1 - Assurer le support utilisateur en centre de service**

1. De nouvelles stations de travail viennent d’être acquises par une entreprise. Cependant les disques sont de capacités insuffisantes. On souhaiterait les remplacer par des disques de 4 To minimum. Quelles sont les précautions et vérifications à prendre avant d’installer le système pour que ces derniers puissent être reconnus ?

On peut :

* Vérifier que le BIOS/UEFI est à jour pour la prise en charge de disques de grande capacité
* Vérifier si le disque est en MBR ou GPT (MBR limite à 2 To, GPT est nécessaire pour exploiter 4 To et plus)
* S’assurer que l’OS prend en charge GPT et UEFI (supporté par les versions “récentes” de Windows 10/11 et Linux Ubuntu)
* Prévoir une sauvegarde des données des anciennes machines
* Vérifier le type d’interface physique sur la carte mère (SATA, NVMe, etc.)

1. Citer différents logiciels permettant de prendre le contrôle à distance d’un équipement numérique et préciser leurs caractéristiques.

* Bureau à distance Windows (Microsoft RDP) : intégré à Windows (client et serveur), logiciel graphique pour prendre le contrôle à distance de matériel sous Windows. Compatible avec d’autres OS si RDP est installé. Accès avec mot de passe, certificat.
* Team Viewer : logiciel utilisant le protocole propriétaire Team Viewer pour prendre la main à distance avec une GUI sur différents OS.
* VNC (Ultra VNC, VNC 32, etc.) : logiciel utilisant le protocole VNC pour un accès graphique sur différents OS. Accès avec chiffrement, mot de passe, téléversement de fichiers possible.
* AnyDesk : logiciel de prise en main à distance très léger, simple d’utilisation. Faible latence, léger, cryptage AES.
* Open SSH : logiciel utilisant le protocole SSH pour une communication en mode texte avec clés de chiffrement asymétrique entre 2 hôtes Unix/GNU Linux. Implémentation sur Windows avec Microsoft Open SH. Utilisation graphique possible avec X11 Forwarding (nativement sur GNU/Linux).

1. Rédiger une note de service sous forme d’un email à destination des utilisateurs de votre entreprise les prévenant d’une opération de maintenance du service SI sur la base de données du serveur d’applications de l’entreprise (pendant cette période, la base de données ne sera pas accessible).

Objet : Opération de maintenance sur la base de données – Interruption temporaire

Pour tous les utilisateurs de la société XXX,

Une opération de maintenance est prévue sur la base de données du serveur d’applications de l’entreprise le XXX. Durant cette période, l’accès à la base de données ne sera pas possible.

Nous vous recommandons d’enregistrer votre travail avant cette maintenance pour éviter toute perte de données.

Nous vous informerons dès que le service sera de nouveau disponible.

Merci de votre compréhension.

Cordialement,

Le Service Informatique

1. Vous devez former les utilisateurs à l’utilisation d’une solution de stockage de fichiers en ligne. Quels sont les points que vous évoquez dans votre document de présentation ?

* Présentation de la solution choisie (ex. : Dropbox, Google Drive, OneDrive, etc.)
* Comment se connecter à la solution, livraison des login/mot de passe
* Comment sauvegarder les fichiers
* Comment partager les documents

1. Quelle procédure est à réaliser pour récupérer un fichier supprimé par un utilisateur sur son ordinateur professionnel ?

* Vérifier dans la corbeille de l’utilisateur
* Vérifier si une sauvegarde est disponible
* Si rien de tout cela ne fonctionne, utiliser des outils de récupération de données

1. Un utilisateur ne peut pas consulter sa messagerie sur son smartphone professionnel. De quels renseignements avez-vous besoin pour lui configurer ?

Voici les renseignements nécessaires :

* Adresse e-mail et mot de passe de l’utilisateur (qui peut être différent de son mot de passe d’accès au système)
* Serveurs entrants et sortants (IMAP/SMTP avec leurs ports et paramètres de chiffrement)
* Configuration spécifique en cas d’authentification forte (2FA, etc.)

1. Après différents tests, vous venez de résoudre un problème remonté par un utilisateur sur son poste de travail. Que devez-vous faire après avoir trouvé cette solution technique ?

* Informer l'utilisateur de la résolution du problème
* Vérifier auprès de l'utilisateur que la solution est bien fonctionnelle
* Mettre à jour le ticket d’incident en indiquant la solution utilisée
* Documenter la solution dans la base de connaissances de l'entreprise

1. Pendant la pause déjeuner, presque tout le personnel de votre entreprise est absent des locaux. Vous devez passer en urgence un correctif de sécurité. Ce correctif demande un redémarrage des ordinateurs clients. Que faites-vous ?

* Faire une communication rapide aux utilisateurs (mail) en précisant le degré d’urgence et l’action qui va être faite (application d’un correctif et redémarrage des postes)
* Appliquer le correctif et forcer le redémarrage des ordinateurs
* Vérifier la réussite de l'application du correctif après le redémarrage des ordinateurs
* Faire une seconde communication aux utilisateurs en donnant le résultat de l’action

1. Dans votre entreprise, les utilisateurs se plaignent de ne pas retrouver leurs fichiers et dossiers sur les “bureaux” des ordinateurs sur lesquels ils se connectent. Ils sont obligés de s’envoyer leurs documents par mail. Comment pouvez-vous faire évoluer cette situation ?

* Mettre en place les profils itinérants sous Windows (stockage du profil sur un serveur)
* Mettre en place un serveur de fichiers réseau ou un espace de stockage cloud (OneDrive, etc.)
* Former les utilisateurs à l'utilisation de ces ressources partagées

**CCP2 - Exploiter des serveurs Windows et un domaine Active Directory**

1. Quels sont les outils disponibles sur les serveurs Windows pour gérer les journaux d'événements ?

* L’observateur d’événements (Event Viewer) : Interface graphique pour afficher, filtrer et exporter les journaux
* PowerShell : avec des commandes comme Get-EventLog ou Get-WinEvent pour interroger et analyser les journaux
* Le système d'abonnement : il permet de centraliser les journaux de plusieurs serveurs sur un même serveur

1. Qu'est-ce qu'une GPO ?

Une GPO (Group Policy Object) est un ensemble de règles dans Active Directory pour gérer et sécuriser les utilisateurs et ordinateurs d’un domaine.

1. Est-ce une bonne pratique de partager des fichiers ou des dossiers sur un partage réseau, en mettant des permissions NTFS sur des utilisateurs ?

Sur le principe oui car :

* Le fait de mettre une ressource sur un partage réseau permet de la rendre accessible aux personnes autorisées
* Le fait d’utiliser les permissions NTFS permet d’affiner les droits (Lecture et Ecriture) sur les objets cibles comme des fichiers ou des dossiers

Néanmoins, c’est une bien meilleure pratique d’utiliser les permissions NTFS sur des groupes d’utilisateurs que directement sur des utilisateurs.

1. Si l'utilisateur jdoe existe sur un domaine Active Directory, sur une machine spécifique, utilisera-t-il le même bureau que l'utilisateur local jdoe ?

Non car ce sont 2 comptes différents :

* Pour le compte jdoe du domaine, son profil est stocké dans C:\Users\jdoe.Domaine
* Pour le compte jdoe en local sur la machine, son profil est stocké sur la machine, dans C:\Users\jdoe, sans aucun lien avec l’Active Directory

Attention, si le compte du domaine se connecte en premier, il utilisera le dossier de profil C:\Users\jdoe.

Il n’est pas recommandé d’avoir des utilisateurs locaux qui portent les mêmes caractéristiques d'identification que des utilisateurs du domaine pour éviter l'écrasement de données locales.

1. Active Directory contient-il une base de données hiérarchique ou relationnelle ? Explique avec au moins un exemple.

Active Directory est une base de données hiérarchique. Exemple avec l’utilisateur jdoe qui est (exemple) dans l’OU DSI, elle-même dans l’OU Utilisateurs, elle-même sous la racine du domaine. Le DistinguishedName de cet utilisateur sera : CN=jdoe,OU=DSI,OU=Utilisateurs, DC=MyLab,DC=fr).

À la différence avec une base de données relationnelle, les objets ne sont pas liés par des clés étrangères, mais par une structure en arbre avec un héritage des permissions et des configurations.

1. Comment mettre en place une politique de mots de passe sur un domaine Active Directory ?

On peut utiliser la GPO “Default Domain Policy” qui permet d’avoir un paramétrage global sur l’AD.

On peut aussi utiliser les FGPP (Fine Grained Password Policies) qui permettent de définir plusieurs stratégies de mot de passe pour différents groupes d’utilisateurs.

1. Qu'est-ce qu'un objet Active Directory ?

Un objet Active Directory est une entité stockée dans la base AD. Il existe plusieurs classes d’objets qui définissent leur nature, comme les utilisateurs, les ordinateurs, les groupes, les OU, etc.

Chaque objet possède un identifiant unique, un SId (au niveau du domaine), et un GUID (au niveau de la forêt).

1. Est-ce une bonne pratique de supprimer un compte utilisateur le lendemain du départ d'un collaborateur d'une société ?

Non ce n’est pas une bonne pratique. Il vaut mieux :

* Désactiver le compte
* Déplacer l’objet utilisateur AD dans une autre OU (de quarantaine)
* Modifier le mot de passe
* Transférer les droits de groupe, de messagerie, etc. si nécessaire
* Programmer (automatiquement ou non) la suppression du compte au bout de 90 jours.

1. Comment gérer l'administration d'un serveur core ?

On peut l’administrer en local, en CLI :

* Avec le menu SConfig
* En ligne de commandes PowerShell ou cmd

Mais également à distance :

* En ligne de commandes PowerShell remote
* Avec du Bureau à distance
* En utilisant la console Server Manager qui permet de prendre la main avec une MMC graphique

**CCP3 - Exploiter des serveurs Linux**

1. Sur les systèmes Linux, avec quel utilitaire peut-on partitionner des disques durs de plus de 2 To ?

Fdisk ne fonctionne pas avec les partitions supérieur à 2 To, donc on peut utiliser (par exemple) gdisk ou gfdisk.

1. Sur un système Linux, que trouve-t'on dans les fichiers /etc/shadow, /etc/passwd, /etc/group ?

Le fichier /etc/shadow contient les mot de passe chiffrés des utilisateurs du système.

Le fichier /etc/passwd contient les informations sur les comptes d’utilisateurs du système.

Le fichier /etc/group contient les informations sur les groupes d’utilisateurs du système.

1. Est-ce que "systemctl start" et "systemctl enable" ont le même effet ?

La commande systemctl est utilisée pour gérer les services sur systemd sur une distribution Linux.

“Systemctl start” démarre un service, alors que “systemctl enable” configure un service pour qu’il démarre automatiquement au boot système.

Donc ces 2 commandes n’ont pas le même effet.

1. Est-ce que la commande dig sur Linux est la même chose que tracert sur Windows ?

La commande dig sur Linux requête des informations sur les DNS, alors que tracert sur Windows donne le chemin (avec les saut de routeurs) des paquets IP vers une destination.

Ces 2 commandes sont donc différentes.

1. Quelle commande permet d'afficher les 20 dernières lignes des logs du système en temps réel ?

tail -n 20 -f /var/log/syslog

1. Que fait la commande suivante : usermod -a -G admin sthomas

La commande “usermod” modifie les caractéristiques d’un compte utilisateur. En l'occurrence, ici la commande complète ajoute l’utilisateur “sthomas” au groupe “admin”. L’option “-a” ne fait pas perdre tous ses groupes à l’utilisateur.

1. Un technicien a exécuté la commande suivante : chmod 777 startScript.sh . Est-ce une bonne idée ?

La commande indiquée donne tous les droits (Lecture, Ecriture, et Execution) sur le fichier startScript.sh, donc non ce n’est pas une bonne pratique.

1. Est-ce que mount et umount sur Linux ont la même fonctionnalité que dism mount et dism umount sur windows ?

Mount et umount sur Linux montent et démontent des systèmes de fichiers.

Dism mount et dism umount sous Windows montent et démontent des images d’OS.

Ces 2 commandes ont des fonctionnalités similaires dans le fait de “monter” un objet sur un OS pour le rendre accessible par la navigation dans une architecture de fichiers. Néanmoins, leurs cibles et leurs utilisations sont différentes, de plus elles sont sur 2 OS différents.

On peut donc considérer qu’elles ne sont pas équivalentes et n’ont pas la même fonctionnalité.

1. A quoi sert Samba sur Linux ? Donne son équivalent sur Windows.

Samba est une implémentation open-source du protocole SMB (équivalent sur les systèmes Windows) pour les systèmes Linux et Unix. Il permet aux ordinateurs non-Windows de se connecter et de partager des fichiers avec des ordinateurs Windows en utilisant le protocole SMB.

**CCP4 - Exploiter un réseau IP**

1. Qu'est-ce qu'une topologie réseau ? Quels sont les 2 types de topologie ?

Une topologie réseau est un type de schéma d’organisation décrivant comment les différents nœuds d’un réseau sont connectés.

Les 2 types de topologies sont la topologie physique (câblage) et la topologie logique (transmission des données).

Les VLANs (Virtual Local Area Networks) font partie des mécanismes permettant d'implémenter des topologies logiques.

1. Donne 5 protocoles courants, avec leur nom, leur fonction, ainsi que leur port par défaut. Donne leur équivalence en mode sécurisé avec les mêmes informations.

Exemple :

HTTP :

* Courant : transfert de pages web sur Internet, port 80
* Sécurisé : HTTPS, port 443

SMTP :

* Courant : envoi de courriels entre clients et serveurs de messagerie, port 25
* Sécurisé : SMTP, port 465

FTP :

* Courant : transfert de fichiers, port 21
* Sécurisé : SFTP, port 22

DNS :

* Courant : résolution de noms de domaine, port 53
* Sécurisé : DNS-over-TLS, port 853

IMAP :

* Courant : synchro. des emails entre un client et un serveur de messagerie, port 143
* Sécurisé : IMAPS, port 993

1. Pour les lignes de commandes suivantes :

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Gi0/1, Gi0/2, Gi0/3, Gi2/0

Gi2/1, Gi2/2, Gi2/3, Gi3/0

Gi3/1, Gi3/2, Gi3/3

2 DSI active Gi0/0

10 FINANCES active Gi1/0, Gi1/1, Gi1/2, Gi1/3

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Que peut-on dire des interfaces Gi0/3, Gi1/2, Gi1/3 ?

Combien y-a-t’il de vlans ?

Gi0/3 est sur le vlan 1 (default).

Gi1/2 et Gi1/3 sont sur le vlan 10 (FINANCES)

On voit 7 id de vlans sur cette copie d’écran. Seuls 3 sont actifs : default, DSI, et FINANCES.

Les 4 autres sont des vlans par défaut “historiques” qui ne sont pas supportés.

1. Qu'est-ce qu'un trunk pour des vlans ?

Un trunk est un moyen de transporter plusieurs vlans sur une même liaison physique (câble réseau). Chaque vlan est identifié par un numéro d’id qui permet d’orienter les trames réseaux vers leurs destinations. Ce dispositif évite la multiplication des matériels réseaux en permettant d’avoir un seul switch au lieu de plusieurs.

1. Quel est l’intérêt de faire des sous-réseaux du point de vue des tables de routage ?

Les sous-réseaux simplifient les tables de routage en regroupant les adresses IP. De plus, cela amène une plus grande segmentation du réseau, donc une meilleure sécurité. Par exemple, un réseau en /25 peut être composé de plusieurs sous-réseaux en /26 ou /27.

1. On a un réseau 132.45.0.0/16. On souhaite découper ce réseau en 8 sous-réseaux.

a. Combien de bits supplémentaires sont nécessaires pour définir ces 8 sous-réseaux ?

b. Quel est le masque correspondant ?

c. Donne l'adresse réseau de ces 8 sous-réseaux.

d. Quelle est l'adresse de diffusion du 4ème sous-réseau ?

a.

On veut découper 132.45.0.0/16 en 8 sous-réseaux. On cherche n tel que 2^n soit supérieur ou égal à 8.

2\*2\*2 = 8 = 2^3 donc n=3.

Il faut 3 bits supplémentaires.

b.

En notation CIDR, le masque est /16, donc avec 3 bits de plus, ça sera /19.

c.

132.45.0.0/19 est la première adresse, donc c’est l’adresse réseau du premier sous-réseau.

Le réseau d’origine est 132.45.0.0/16, et cela amène des sous-réseaux en /19, donc il n’y a que les 3ème et 4ème octet qui vont être modifiés.

Le 3ème octet va de 0 à 256, et 256/8 = 32, donc Pour le 1er sous-réseau :

Adresse de réseau : 132.45.0.0/19

1ère adresse disponible : 132.45.0.1

Dernière adresse disponible : 132.45.31.254

Adresse de broadcast : 132.45.31.255

Pour les autres sous-réseaux, l’adresse de réseau est :

Sous-réseau 2 : 132.45.32.0/19

Sous-réseau 3 : 132.45.64.0/19

Sous-réseau 4 : 132.45.96.0/19

Sous-réseau 5 : 132.45.128.0/19

Sous-réseau 6 : 132.45.160.0/19

Sous-réseau 7 : 132.45.192.0/19

Sous-réseau 8 : 132.45.224.0/19

d.

L’adresse de diffusion (broadcast) du 4ème sous-réseau est 132.45.127.255