Projet BALSAN

I) Le contexte Balsan

La société de confection Balsan est implantée à MontierChaume. Elle est le fournisseur de tradition de l'armée française depuis 1850. Ainsi, Balsan est devenue l'un des principaux fabricants français d'uniformes. Balsan développe des outils informatiques et logistiques performants et adaptés à des collections d'articles très larges en nombre et en gammes. Balsan répond ainsi aisément aux besoins d'externalisation de l'habillement.

Mais si les outils informatiques dédiés à la confection et au patronage des uniformes sont à la pointe du progrès, en revanche, son infrastructure système, réseau, et sécurité n'a que peu évolué depuis que Balsan a intégré ses locaux de MontierChaume. Et tant les incidents que les demandes des clients ou des employés s'accumulent. En fait, il n'existe pas vraiment de service informatique : c'est le chef-comptable qui assure tant bien que mal, en plus de ses fonctions principales, la charge de gérer l'informatique a minima.

II) L'existant au niveau technique

A votre arrivée, un schéma physique du réseau informatique tel qu'il existe à ce jour vous est fourni :

Un seul réseau IPv4 en 192.168.*1*.0/24 a été mis en place et toutes les stations de travail fonctionnent sous Windows 11 *Professional* en adressage IP statique. Aucun serveur de fichiers, d'authentification, de résolution de nom n'a encore été implémenté. Seul un PC équipé de Windows 11 Pro et d'un disque dur de 1To fait office de partage de fichiers à travers un simple groupe de travail (*WorkGroup*), ce qui est loin de représenter une situation souhaitable dans un cadre d'entreprise ; cette situation est très éloignée de celles recommandées par les référentiels de bonnes pratiques comme ITIL-v4.

Remarque pédagogique : en milieu professionnel, il n'est évidemment pas question d'utiliser pour les stations de travail utilisées par les salariés des systèmes conçus pour le milieu familial qui ne disposent pas de toutes les fonctions offertes par les systèmes professionnels. Ainsi, vous ne devrez JAMAIS installer durant votre parcours de BTS des versions de Windows 11 *Home* ou *Family* qui sont trop limitées ; idem pour Windows 10. En revanche, vous devrez systématiquement choisir les versions *Professional* ou *Enterprise* soit de Windows 10, soit de Windows 11 pour vos installations de stations de travail-tests. Quant aux serveurs, vous devrez impérativement opter pour des systèmes d'exploitation spécifiquement développés pour des tâches lourdes (distribution de services) dédiées aux serveurs : Linux (Debian 11 par exemple), ou Windows 2019 ou 2022 *Server*.

III) Les problèmes constatés

Profitant du fait que vous êtes stagiaires en informatique, le chef-comptable vous demande de mener une étude qui doit permettre de mieux répondre aux défaillances techniques vécues, aux incidents survenus, aux défauts de sécurité ainsi qu'aux problèmes vécus quotidiennement par les utilisateurs du réseau, ceci afin de se

rapprocher petit à petit des recommandations faites par le référentiel de bonnes pratiques ITIL-v4.

- au niveau matériel...
  - Depuis deux ans, plusieurs pannes, incidents, et défaillances ont eu lieu :
    - Le disque dur de l'ordinateur faisant office de partage de fichiers est tombé en panne totale : aucun fichier n'a pu être récupéré. Quasiment tous les salariés de l'entreprise ont été bloqués pendant près d'une journée (ce qui a représenté la perte de près de 18.700 € d'arrêt de production !) le temps d'acheter un nouveau disque dur de remplacement, de le reconnecter à l'intérieur de l'unité centrale, de réinstaller Windows 11 Professionnel, puis de restaurer une sauvegarde (trop ancienne) des fichiers partagés.
      => Selon vous, quel type de système ou technologie aurait pu permettre d'éviter un tel crash ?
    - Aucun dispositif de sauvegarde régulier n'ayant été mis en place, les sauvegardes sont réalisées (parfois - lorsqu'il y pense ou qu'il a le temps... !) par le chef comptable sur ... DVD-RW ! Bref, rien de régulier, ni de pertinent, ni d'efficace, ni de fiable... Ce type de procédé est aujourd'hui à bannir totalement du domaine professionnel.
      => Connaissez-vous des solutions fiables qui permettraient à l'avenir de sécuriser les données vitales d'une entreprise de taille moyenne comme Balsan disposant d'un maigre budget destiné à l'informatique ?
  - Erreurs humaines :
    - Après avoir changé le très vieil ordinateur du service logistique, le chef comptable a voulu re-paramétrer la configuration IP de cette machine, en lui attribuant l'adresse IPv4 192.168.1.12, le masque de sous-réseau 255.255.255.0, et la passerelle 192.16.1.254. Le responsable logistique qui avait auparavant accès à internet lui explique que depuis le changement d'ordinateur, il ne peut plus ouvrir sa boite mail et qu'il n'a plus accès à internet, alors qu'il peut toujours ouvrir ou enregistrer des fichiers dans l'espace partagé de l'ordinateur PC0-PartageDeFichiers. Il ne comprend pas pourquoi, n'étant pas spécialiste.
      => Et vous, qu'en pensez-vous ?
    - Lorsqu'un visiteur extérieur vient en rendez-vous chez Balsan, c'est souvent avec son propre ordinateur portable qui contient en général tous les catalogues de produits, les références des fournisseurs accessibles par internet, ... Mais pour disposer chez Balsan d'un accès à internet, il faut se connecter au réseau local de Balsan. Et pour cela, il est nécessaire de demander au visiteur d'entrer manuellement en tant qu'administrateur de son portable, tous les paramètres IP notés sur un petit papier collé au coin d'une table de la salle de réunion (!). Peu pratique, et surtout, nombreux sont les visiteurs qui ne savent pas comment procéder, voire qui ne disposent pas des droits administrateurs sur leur système d'exploitation de leur portable d'entreprise. Ce mécanisme est donc peu adapté.
      => Quelle solution technique pourriez-vous proposer pour ne plus avoir à gérer ce type de problème technique ?

- au niveau de la sécurité...
    - Toutes les machines se trouvant dans le même réseau IP, chaque ordinateur peut potentiellement avoir accès à n'importe quel autre ordinateur du réseau, en fonction des faiblesses éventuelles des pares-feux locaux, ce qui représente un grave manquement aux règles de base en matière de sécurité. Certains salariés indélicats ont d'ailleurs déjà pu récupérer des documents parfois confidentiels, stockés de manière plus ou moins partagée sur plusieurs ordinateurs de différents services, générant des conflits humains à l'intérieur de l'entreprise.
      => Quelle solution efficace faudrait-il mettre en place pour proposer de véritables espaces de stockage partagés centralisés mais sécurisés selon des droits attribués à chaque utilisateur ?
      => Comment faire pour que chaque utilisateur dispose malgré tout d'un espace privé de stockage, bien à lui, mais sécurisé et régulièrement sauvegardé, même si ce salarié est amené à changer de station de travail ?
    - Par ailleurs, à ce jour, n'importe qui peut démarrer n'importe quel ordinateur de Balsan, et accéder à toutes les ressources du réseau sans avoir jamais à fournir aucun *login* et mot de passe. Ceci est une faille de sécurité majeure que des anciens salariés indélicats avaient déjà exploité à plusieurs reprises il y a quelques mois en arrière. Aucune gestion centralisée et sécurisée des accès au réseau n'est opérée à ce jour. Il est même déjà arrivé qu'un salarié qui n'avait pas reçu l'augmentation de salaire qu'il espérait, et qui disposait d'une clé d'accès au bureau de la logistique soit venu un dimanche matin pour se connecter à l'ordinateur logistique, et ait détruit plusieurs centaines de fichiers importants utilisés par la Direction, et probablement récupéré de nombreux autres fichiers sur un disque USB externe. L'impact financier a été énorme pour l'entreprise qui depuis souhaite mettre en œuvre des solutions efficaces pour ne plus revivre ça à l'avenir.
      => Vous, que proposeriez-vous ? Comment faire, selon vous, pour gérer la sécurité des accès aux machines et donc aux ressources du réseau de Balsan, en prenant en compte des plages horaires de présence des salariés ?

- au niveau des demandes des utilisateurs du réseau...
    - Lorsque des commerciaux (fournisseurs) ou techniciens (d'entreprises sous-traitantes) viennent dans les locaux de Balsan pour effectuer des interventions en tant que partenaires, ils ont de plus en plus fréquemment un besoin capital de pouvoir accéder à l'internet à partir de leurs propres ordinateurs portables. Pour pouvoir accéder aux ressources des ordinateurs locaux ou de serveurs présents sur le web, il est bien plus naturel de les joindre par leur nom d'ordinateur. Or, si aucun protocole particulier de résolution de nom n'est activé, cela reste impossible : il faut alors taper l'adresse IP de la machine ou du serveur Web à contacter (qu'en général, personne ne connaît, en dehors de quelques informaticiens !). Ceci est absolument impensable à exiger de la part de salariés qui ne connaissent que très peu le monde informatique et qui doivent être efficaces dans leur travail : il est impératif qu'ils puissent accéder à des ressources par leur nom, de manière mnémotechnique, et surtout pas par leur adresse IP.

=> Quel protocole et quel type de solution connaissez-vous, qui pourraient répondre à cette problématique ?

IV) Les solutions à envisager pour répondre aux besoins "clients"

- Pour assurer une tolérance de pannes au niveau des espaces de stockages "critiques" (très importants pour l'entreprise) car partagés par l'ensemble des salariés pour des tâches quotidiennes et capitales pour l'activité principale, prévoir d'utiliser sur un véritable système serveur Windows 2019 *Server* (installé dans une machine physique mais aussi de préférence sur une machine virtuelle, plus facilement adaptable) au moins 2 disques durs (physiques, ou virtuels si le serveur est virtuel) montés avec l'une des technologies RAID (RAID 1 dans un premier temps), afin que si 1 disque *crashe*, l'autre (ou les autres) puisse continuer d'assurer sa fonction de stockage de fichiers de manière transparente pour tous les utilisateurs.
- Dans ce serveur ("Serveur-A : PartageSIO"), prévoir sur l'espace de stockage à tolérance de pannes, 2 partitions :
    1. partition (C:) réservée au système d'exploitation, aux services de serveur, ainsi qu'aux quelques applications (25 Go)
    2. partition (P:) réservée au partage des données des salariés ainsi qu'aux dossiers personnels de chaque salarié (10 Go).
- Par mesure de sécurité, et afin que les données sauvegardées ne soient pas stockées dans la même machine que les données elles-mêmes (risque de corruption par virus, ...), l'achat d'une 2ème licence Windows 2019 Server est finalement prévue dans le but d'installer un 2ème serveur (virtuel) ("Serveur B : SauveSIO") lui aussi équipé de 2 disques montés en RAID1 pour effectuer automatiquement, régulièrement et recueillir les sauvegardes des données partagées, des données individuelles des salariés (venant du Serveur A), mais aussi des autres systèmes serveurs (Serveur A, Serveur C, ...), afin d'être bien plus efficace en cas de défaillance majeure. Compte-tenu du coût d'achat des licences Windows Server (renseignez-vous un peu du coût d'une telle licence... => Combien pour 1 licence Windows 2019 *Server Standard Edition* ? .....), des disques, des machines supportant la virtualisation, etc.,
  => Etudiez les différentes solutions de sauvegardes et proposez une application de sauvegarde adaptée (la moins onéreuse possible), à condition qu'elle demeure réellement utilisable pour des usages professionnels (ex : Cobian Backup, Veem Backup, ...).

- Ce second serveur sera affecté d'un espace de stockage à tolérance de pannes constitué de 2 partitions :
    - partition (C:) réservée au système d'exploitation ainsi qu'à l'application de gestion des sauvegardes automatisées (20 Go)
    - partition (S:) réservée au recueil des fichiers de sauvegarde (25 Go). Au niveau des sauvegardes, il va être nécessaire d'établir un plan de sauvegarde pertinent et différencié selon les éléments qui sont à sauvegarder : on ne sauvegarde pas de la même manière, avec la même fréquence, et au même endroit les éléments faisant partie du cœur du

système d'exploitation, des logiciels, ou des données utilisateurs ou logicielles qui elles se modifient tous les jours.

- Le mieux est de présenter sous forme de tableau ce plan de sauvegarde :

Eléments à sauvegarder	Méthode de sauvegarde	Fréquence de sauvegarde	Lieu de destination de sauvegarde
ex : PartageSIO : O/S	complète	1 fois / semestre	\\SauveSIO\Sauvegardes\SrvA\OS
ex : PartageSIO : Partages	Complète incrémentielle	1 fois / semaine (samedi 22:00) 1 fois / jour (21:00)	\\SauveSIO\Sauvegardes\SrvA\data
ex : MaitreSIO : O/S	complète	1 fois / semestre	\\SauveSIO\Sauvegardes\SrvC\OS
ex : MaitreSIO : services	complète	1 fois / mois	\\SauveSIO\Sauvegardes\SrvC\services
ex : MaitreSIO : données	Complète incrémentielle	1 fois / semaine (samedi 23:30) 1 fois / jour (21:30)	\\SauveSIO\Sauvegardes\SrvC\data

- Remarque pédagogique : Les données à l'intérieur de ce tableau ne vous sont fournies qu'à titre d'exemple et doivent être adaptées par vous en bonne intelligence, en fonction de chaque cas rencontré dans chaque entreprise.
  Une fois que, pour chaque serveur à sauvegarder, vous avez établi ce plan de sauvegarde, à vous de programmer les tâches de sauvegardes qui vont permettre la réalisation effective et automatisée de ces sauvegardes.

Remarque pédagogique : n'oubliez-pas de contrôler que toutes les sauvegardes réalisées sont bel et bien opérationnelles, et prévoyez de provoquer un *crash* d'un (ou plusieurs) serveur(s) pour tester une restauration, et vous assurer que votre "filet de sécurité" est effectivement pleinement opérationnel (et accessoirement,... que vous ne serez pas licencié de votre emploi pour faute grave ;-) !!!).

- Afin de régler pour de bon les problèmes de failles majeures de sécurité dues à l'absence totale de contrôle des accès au réseau, aux machines, aux dossiers partagés, etc., la mise en œuvre d'un contrôleur de domaine semble inéluctable. Si dans un 1er temps, il a été envisagé pour des raisons d'économies, de faire installer ce type de service sur le serveur de stockage déjà équipé de Windows 2019 *Server* (Serveur A), il paraît finalement bien plus prudent de laisser ce 1er serveur A totalement isolé des autres, du fait du risque majeur de corruption potentielle (rappelons que ce serveur A va héberger des fichiers venant des salariés, et donc potentiellement infectés, ce qui risque de corrompre à tout moment l'ensemble du serveur et des services associés). Aussi, et malgré le coût que représente l'achat d'une 3ème licence Windows *Server* 2019 ainsi que l'investissement dans une nouvelle machine (même virtuelle !), décision est prise de vous laisser libre de réaliser cette installation d'une 3ème licence Windows 2019 *Server* sur une 3ème VM (Serveur C : MaitreSIO) elle aussi équipée d'un système de stockage à tolérance de pannes (type RAID 1), et d'y installer le service (rôle) de contrôleur de domaine ActiveDirectory (AD-DS) basé sur la zone de nommage *balsan.fr* qu'il va falloir créer. Grâce à ce contrôleur de domaine, vous allez pouvoir gérer :
  - chaque utilisateur en lui créant un compte individuel de connexion (login + mot de passe fort)
  - des groupes (Direction, comptabilité, informatique, logistique, production, visiteur) en affectant chaque utilisateur à l'un de ces groupes
  - des droits d'accès aux ressources du domaine *balsan.fr* pour chacun de ces groupes, ou par utilisateur
  - l'affectation d'un accès par unité logique (ex : Z:) à un dossier individuel centralisé sur serveur de partage (Serveur A) pour chaque utilisateur (pensez à utiliser la variable système $USERNAME$ dans le nom du chemin à attribuer).
  - des plages horaires durant lesquelles la connexion est possible, groupe par groupe :
    - Groupes Direction et informatique : accès 7j/7 de 6:00 à 23:00 ;
    - Groupes comptabilité et visiteur : accès du lundi au vendredi de 8:00 à 13:00 et de 14:00 à 19:00 ;
    - Groupe logistique : accès du lundi au vendredi de 7:00 à 15:00 ;
    - Groupe production : accès du lundi au vendredi de 8:00 à 18:00.
  - l'intégration des 2 autres serveurs (Serveur A et Serveur B) dans le domaine *balsan.fr*.
- Concernant les problèmes d'accès aux ressources par leur nom, il est fondamental d'y remédier par la mise en œuvre d'un service DNS (service de résolution de nom). Ce service a déjà été partiellement installé lors de la création du domaine et de l'installation du contrôleur de domaine par Active Directory (AD-DS) sur le Serveur C : MaitreSIO. Il ne reste plus qu'à finir de le paramétrer en s'assurant que les deux autres serveurs A et B sont bien enregistrés tant dans la zone de recherche directe (*balsan.fr*) que dans la zone de recherche inversée (à créer le cas échéant). Mais ce serveur ne saura pas résoudre tous les noms de tous les serveurs de l'internet,

et il est illusoire pour vous de tous les enregistrer ici manuellement (à moins que vous ne disposiez de 10 ou 12 vies devant vous ! ...). Vous allez donc indiquer à votre service DNS l'adresse IP d'un redirecteur (un autre serveur DNS qui lui, serait en mesure de résoudre ces noms de serveurs présents sur le web) ; vous pouvez indiquer des serveurs "publics" comme ceux de *Free.fr* par exemple (=> d'après vous, quels sont les deux principaux serveurs DNS proposés par Free que vous pourriez utiliser ici en tant que redirecteurs ? ..... et .....).

- Pour régler les problèmes dus aux erreurs humaines survenues, la mise en œuvre d'un service DHCP semble là-encore inéluctable, pour faire distribuer dynamiquement et automatiquement à des ordinateurs se connectant au réseau de Balsan, tout le lot nécessaire de paramètres IP (y compris l'adresse de la bonne passerelle de sortie du réseau). En tant qu'administrateur système responsable et soucieux d'utiliser les ressources avec parcimonie, vous ne pouvez pas prendre l'initiative d'ajouter encore un nouveau serveur supplémentaire (un 4ème ? !!!), équipé d'un nouveau système d'exploitation serveur, juste pour mettre en œuvre un nouveau service de ce type. Dans ce cas particulier, il est recommandé d'utiliser le serveur (Serveur C : MaitreSIO) faisant office de contrôleur de domaine et de serveur DNS pour y installer le service de DHCP qui pourra proposer une distribution automatisée d'adresses IP sur une étendue allant de 192.168.*1*.10/24 à 192.168.*1*.30/24, ainsi que de la passerelle adéquate. Il faudra bien entendu autoriser ce serveur au niveau du contrôleur de domaine (seul l'administrateur du domaine est autorisé à le faire) afin que n'importe qui ne vienne pas perturber le fonctionnement du réseau avec l'ajout cavalier d'un serveur DHCP sauvage.

- => Il est conseillé de s'assurer d'une continuité de service avec par exemple l'analyseur de trame Wireshark.

V) Les nouveaux matériels envisagés par investissement

Si l'on résume :

- 3 nouvelles machines de type serveur peuvent être achetées ou récupérées (voire virtualisées selon les contraintes spécifiques au lycée) :
  - Un nouveau serveur (Serveur A PartageSIO) équipé de Windows 2019 Server va être ajouté à l'infrastructure existante en remplacement du poste Windows 11 de partage actuellement utilisé. Il va héberger le service de partage de fichiers pour toute l'entreprise Balsan, ainsi que les dossiers individuels de chaque utilisateur du domaine.
  - Un deuxième nouveau serveur (Serveur B SauveSIO) équipé de Windows 2019 Server sera chargé de réaliser, ainsi que d'héberger les sauvegardes de tous les autres serveurs.
  - Un troisième nouveau serveur (Serveur C MaitreSIO) équipé lui aussi de Windows 2019 Server sera chargé des rôles de contrôleur de domaine, de serveur DNS, et de serveur DHCP pour l'ensemble du domaine *balsan.fr*.

=> Et maintenant, évaluez le coût total des investissements réalisés pour optimiser et sécuriser à minima le système d'information de Balsan :

- au niveau matériel (ou équivalent virtuel) : TOTAL :
- au niveau système : TOTAL :

- au niveau service : TOTAL :
- au niveau logiciel : TOTAL :
- au niveau des éléments de sécurité : TOTAL :
- au niveau du coût relatif au temps passé par l'équipe (base charges comprises : 20€/h/pers.). TOTAL :
- au niveau prestation de service achetée TOTAL :
- TOTAL GÉNÉRAL :

VI) Déroulement du projet

=> Nommez un chef de projet au sein de l'équipe en vue de coordonner les membres de l'équipe et les tâches du projet.

=> Réalisez un inventaire de la configuration matérielle des machines du réseau à l'aide d'une solution adaptée (vous proposerez une procédure d'installation et de configuration de la solution choisie). Dans l'idéal, cette solution s'adaptera facilement à GLPI.

Vous appliquerez une gestion de projet rigoureuse :

=> via Trello, l'outil de gestion de projet en ligne, inspiré par la méthode Kanban apportant un suivi visuel des différentes tâches du projet tout en précisant la répartition des ressources par tâches du projet,

=> en mettant en place un diagramme de Gantt pour afficher des informations visuelles sur le calendrier du projet.

Pensez à effectuer des copies d'écrans tout au long du projet pour compléter votre dossier.

N'oubliez pas de réaliser régulièrement des snapshot de votre machine dans VirtualBox.