

19/11/2025

Compte-rendu

Rendu du cahier des charges

Fait par : Mattéo Mouranchon – Groupe 2

Contexte du rapport

Le laboratoire **Galaxy Swiss Bourdin (GSB)** est le résultat d'une fusion stratégique entre deux acteurs majeurs de l'industrie pharmaceutique. D'un côté, **Galaxy**, géant américain reconnu pour son expertise dans le domaine des maladies virales telles que le SIDA, les hépatites et d'autres pathologies infectieuses. De l'autre, **Swiss-Bourdin**, un conglomérat européen regroupant plusieurs laboratoires spécialisés dans la production de médicaments courants et le développement de traitements thérapeutiques plus traditionnels.

Cette union, motivée par la volonté de renforcer leur position sur le marché mondial, a donné naissance à un groupe pharmaceutique puissant, combinant **innovation scientifique, capacité de production et réseau commercial étendu**. Toutefois, la fusion a également mis en évidence de nombreux défis organisationnels, notamment en matière de **gestion du personnel**, de **coordination des services** et surtout d'**harmonisation des outils de travail**.

Après deux années de réorganisation interne, GSB a constaté que les visiteurs médicaux - acteurs essentiels pour la promotion des produits et le lien avec les professionnels de santé - utilisaient des équipements informatiques hétérogènes et souvent obsolètes. Certains étaient dotés de matériel fourni par l'entreprise Galaxy, tandis que d'autres recevaient une indemnité bisannuelle pour s'équiper eux-mêmes selon la politique Swiss-Bourdin. Cette absence d'uniformité compliquait non seulement la maintenance, mais également la **sécurisation des données**, la **remontée d'informations terrain**, et l'**organisation des échanges avec les différents services du siège**.

Question 1 : Spécifications techniques des ordinateurs portables

L'entreprise GSB reverse aux visiteurs une indemnité pour s'équiper en informatique ou comme une donation pour donner de l'impression aux clients.

Pour un usage professionnel de manière intensif, 3 ordinateurs de type vont être recommandés qui vont remplir les conditions suivantes :

- L'ordinateur doit être robuste.
- Le poids de l'ordinateur doit être dans des conditions acceptables, pas trop lourd.
- Être utilisé dans des usages terrain intensifs.
- Avoir une autonomie importante.

Voici les 3 modèles : Lenovo ThinkPad, Dell Latitude et HP EliteBook

Quel modèle d'ordinateur portable recommandez-vous et pourquoi ?

Le HP EliteBook 14 pouces est recommandé, car c'est un ordinateur professionnel, robuste, léger et adapté aux déplacements fréquents.

Quelle est la configuration minimale requise ?

- Un Intel Core i5 minimum.
- 16 Go de RAM.
- Un SSD d'au moins 512 Go.
- La batterie doit avoir au moins 8 heures d'autonomie.

Quel poids maximum ne doit pas être dépassé ?

1,5 kg maximum accepté.

Question 2 : Sécurité et protection des données.

Quel système de chiffrement recommandez-vous ? Pourquoi ?

BitLocker est fortement recommandé, ce système de chiffrement est intégré à Windows, car il est **fiable, simple à activer** et permet de protéger toutes les données de l'ordinateur en cas de perte ou de vol. Attention à se souvenir de ses mots de passe principal car même l'entreprise elle-même ne pourra pas vous aider.

Comment gérez-vous les clés de récupération ?

Les clés de récupération doivent être **sauvegardées dans un espace sécurisé**, par exemple dans un **compte Microsoft professionnel** ou dans un **coffre-fort numérique** de l'entreprise. Elles ne doivent jamais être stockées sur le PC lui-même. En cas de perte ou d'oubli de votre mot de passe, veuillez contacter votre responsable pour faire une récupération.

Comment assurer la séparation données pro/perso ?

Il faut utiliser **deux espaces séparés** :

- Un **compte professionnel** pour les données de l'entreprise, réservé que pendant le travail professionnel.
- Un **compte personnel** ou un **conteneur séparé** pour les fichiers privés et personnelle. Cela évite ainsi toute confusion ou fuite accidentelle.

Quelle procédure en cas de perte ou vol ?

En cas de perte ou de vol, il faut **déclarer immédiatement l'incident au service informatique**, qui pourra :

- Bloquer l'accès aux comptes.
- Déclencher un **effacement à distance** si possible.
- Utiliser BitLocker pour empêcher l'accès aux données.

Comment empêcher l'installation de logiciels non autorisés ?

On peut activer les **Politiques de Sécurité Windows (GPO)**, qui bloquent l'installation de logiciels sans autorisation.

On peut aussi utiliser un **antivirus professionnel** et limiter le PC à des **droits utilisateurs**, empêchant l'installation de programmes inconnus.

Question 3 : Déploiement de 450 postes

Quelle solution de masterisation recommandez-vous ? Pourquoi ?

Je recommande d'utiliser une solution de déploiement automatisé comme **WDS (Windows Deployment Services)**, car elles permettent de créer une image système unique et de la déployer rapidement sur un grand nombre d'ordinateurs.

Source : <https://learn.microsoft.com/fr-fr/windows/win32/wds/windows-deployment-services-portal>

Quelle procédure de test après déploiement ?

Après le déploiement d'un poste, une procédure de test complète doit être effectuée avant la remise à l'utilisateur. Elle comprend :

1. Vérifie que le démarrage Windows fonctionne correctement et que Windows soit actif.
2. Tester la connexion du réseau via l'invite de commande et vérifier que le poste reçoit bien les paquets entre lui et le serveur.
3. Vérifie que les applications les plus utilisées fonctionnent correctement au bon fonctionnement.
4. Vérifier que Windows soit bien à sa dernière version.
5. Vérifier que toute la sécurité du poste soit active, en partie BitLocker, la présence de l'antivirus et le paramétrage recommandé.
6. Répéter les 5 étapes sur les 450 Postes/Machines à déployer.

Comment mettre à jour l'image de déploiement ?

Afin de mettre à jour l'image, veuillez :

1. Prends un PC modèle.
2. Installe les nouvelles version mises à jour et logiciels.
3. Vérifie que tout fonctionne.
4. Re-capture l'image dans WDS.
5. La redéployé lors des prochaines installations.

Question 4 : Connectivité et accès aux ressources

Je recommande une solution **SSL-VPN** ou **IPsec** fournie par un équipement professionnel comme **Fortinet (FortiClient)**, **Cisco AnyConnect**, ou **OpenVPN Access Server**.

Ces solutions offrent :

- Un haut niveau de sécurité.
- Une connexion stable.
- Une authentification forte (mot de passe + MFA),
- Et une compatibilité avec Windows.

Elles permettent aux visiteurs médicaux d'accéder aux ressources internes depuis n'importe où.

Comment configurez-vous l'accès Wifi sécurisé ?

Pour sécuriser le Wifi, il faut mettre en place un réseau décidé pour l'entreprise en version **WPA2-Enterprise** ou **WPA3-Enterprise**, qui utilise :

- Une authentification par identifiant professionnel (**RADIUS**).
- Un mot de passe fort ou un certificat (Bitlocker).
- Et une connexion automatique sur les postes configurés.
Cette méthode évite que le mot de passe Wifi circule et cela garantit que seuls les appareils autorisés peuvent se connecter sans problème.

Quelle sont les politiques pour les connexions WiFi publiques ?

Pour les WiFi publics (cafés, hôtels, transports), les règles sont simples :

- Le **VPN** obligatoire dès la connexion.
- Interdiction d'accéder à des données sensibles sans **VPN** ou en cas de non VPN installé, veuillez ne pas vous connecter.
- Bloqué les sites ou services dangereux.
- Activer l'antivirus et le pare-feu Windows.

Cela protège contre les risques fréquents : écoute du trafic, faux hotspots, vol de données, fuite de donnée, etc.

Comment garantir l'accès aux ressources internes ?

L'accès se fait via :

- Le **VPN**, qui va créer un tunnel sécurisé (ex : Cloud FLARE).
- Une authentification forte (**MFA**) pour vérifier l'identité de l'utilisateur,
- Des **règles réseau** qui autorisent uniquement les applications internes nécessaires (CRM, intranet, messagerie...).
Cela garantit que seuls les utilisateurs autorisés accèdent aux ressources de l'entreprise.

Quel sont les impacts du VPN sur les performances ?

Le VPN peut :

- Réduire légèrement le **débit Internet**.
- Augmenter de peu la **latence**.

Parce que, il chiffre toutes les données et les fait passer par un serveur sécurisé (ex : Nord VPN).

Cependant, sur une bonne connexion 4G/5G ou WiFi, l'impact est **faible** et n'empêche pas le bon fonctionnement des applications métier.

Question 5 : Gestion et remontée des données

Quelles données doivent être sauvegardées automatiquement ?

Les données à sauvegarder automatiquement en backup sont :

- Les documents professionnels (rapports, comptes-rendus).
- Les fichiers liés aux applications métier.
- Les données synchronisées (notes, formulaires, tableaux).
- Et les paramètres importants de l'utilisateur.

L'objectif est que rien d'important ne soit perdu en cas de panne, d'erreur ou de perte de données.

Quelle fréquence de sauvegarde est recommandez ?

Il est recommandé de faire une sauvegarde **quotidienne**, voire **en temps réel** grâce à une synchronisation automatique (comme OneDrive Entreprise).

Cela garantit que les fichiers sont toujours à jour et que il n'est pas d'oublie de la part du service informatique.

Où sont stockées les sauvegardes auxiliaires ?

Les sauvegardes auxiliaires sont stockées :

- Dans le **cloud professionnel de l'entreprise** (OneDrive Entreprise).
- Et dans les **serveurs sécurisés** de l'entreprise.
Ce stockage externe protège les données est utile si l'ordinateur est perdu ou en panne.

Comment restaurer les données en cas de panne ?

En cas de panne :

1. Veuillez réinstalle l'ordinateur avec l'image système.
2. L'utilisateur doit se reconnecte à son compte professionnel.
3. Les fichiers se **relyncheront automatiquement** depuis **OneDrive** ou le **serveur de l'entreprise**.
Il retrouve ainsi toutes ses données perdues sans manipulation complexe. Avant de faire de procédé, veuillez contacter votre administrateur pour procéder à la restauration des données.

Comment assurer la remontée des informations terrain ?

Pour assurer la remontée des informations terrain, on utilise :

- La synchronisation automatique via le **OneDrive**.
- Une connexion stable (Wifi, 4G/5G, VPN si nécessaire).
- Et des logiciels métiers configurés pour envoyer les données dès qu'Internet est disponible.

Ainsi, les données collectées en visite remontent automatiquement au siège social.

QCM

Résultat du QCM

Score : 18/20



Pourcentage : 90%

Date : 19/11/2025

Réponse aux questions QCM

Question 1 :

Question 1

Où se trouve le siège administratif de GSB Europe ?

A. À Philadelphie, États-Unis

B. À Paris, France

C. À Zurich, Suisse

D. À Londres, Royaume-Uni

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 2 :

Question 2

Quel étage du bâtiment abrite la salle serveur chez GSB ?

A. Le rez-de-chaussée

B. Le 3ème étage

C. Le 6ème étage

D. Le sous-sol

Réponse correcte : C

Votre réponse : C ✓ Correct

Question 3 :

Question 3

Combien de visiteurs médicaux GSB compte-t-il en France métropolitaine ?

A. 250

B. 380

C. 480

D. 550

Réponse correcte : C

Votre réponse : C ✓ Correct

Question 4 :

Question 4

Quel est le format des adresses de messagerie chez GSB ?

A. nomUtilisateur@gsb.com

B. nomUtilisateur@swiss-galaxy.com

C. prenom.nom@gsb-europe.com

D. nomUtilisateur@galaxy-swiss.com

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 5 :

Question 5

Quelle technologie est utilisée pour segmenter le réseau chez GSB ?

A. Sous-réseaux IP

B. VLAN

C. DMZ

D. VPN

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 6 :

Question 6

Quel est l'adressage IP du VLAN 'Serveurs' ?

A. 192.168.10.0/24

B. 172.16.0.0/24

C. 10.0.0.0/24

D. 192.168.100.0/24

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 7 :

Question 7

Quel VLAN est dédié aux visiteurs avec un accès limité à Internet uniquement ?

A. VLAN 10

B. VLAN 100

C. VLAN 150

D. VLAN 200

Réponse correcte : C

Votre réponse : C ✓ Correct

Question 8 :

Question 8

Quel service assure le routage inter-VLAN chez GSB ?

A. Le routeur principal

B. Le commutateur MUTLAB

C. Le serveur DHCP

D. Le pare-feu

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 9 :

Question 9

Comment les données de l'entreprise sont-elles sauvegardées ?

A. Sur bandes magnétiques stockées sur site

B. Dans le cloud public

C. Répliquées quotidiennement aux États-Unis par un lien dédié

D. Sur des disques durs externes

Réponse correcte : C

Votre réponse : C ✓ Correct

Question 10 :

Question 10

Quelle est la politique d'équipement informatique des visiteurs médicaux ?

A. Tous reçoivent le même ordinateur portable de l'entreprise

B. Ils reçoivent une indemnité bisannuelle ou une dotation en équipement

C. Ils doivent utiliser leurs appareils personnels

D. Ils n'ont pas d'équipement informatique fourni

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 11 :

Question 11

Quel est le principal objectif de la modernisation de l'activité de visite médicale ?

A. Réduire les coûts de déplacement

B. Améliorer le suivi de l'activité de visite

C. Remplacer les visiteurs par des outils numériques

D. Centraliser toutes les décisions au siège

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 12 :

Question 12

Quel service est responsable de la configuration réseau chez GSB ?

A. Le service Développement

B. Le service Réseau et Système

C. Le service Commercial

D. La Direction des Services Informatiques (DSI)

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 13 :

Question 13

Quelle est la particularité de la salle 'Démonstration' ?

A. Elle est réservée aux réunions de direction

B. Elle dispose de paillasses et d'équipements de laboratoire

C. Elle est équipée de bornes WiFi haute performance

D. Elle héberge les serveurs principaux

Réponse correcte : B

Votre réponse : A X Incorrect

Question 14 :

Question 14

Comment sont sécurisés les accès à la salle serveur ?

A. Par un système de reconnaissance faciale

B. Par un gardien présent 24h/24 et des accès contrôlés

C. Par des caméras de surveillance uniquement

D. Par des portes verrouillées avec code numérique

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 15 :

Question 15

Quelle est la principale fonction du commutateur MUTLAB ?

A. Fournir une connexion Internet redondante

B. Assurer le routage inter-VLAN avec des ACL

C. Gérer les sauvegardes des serveurs

D. Contrôler l'accès WiFi des visiteurs

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 16 :

Question 16

Quels services peuvent être accessibles depuis le VLAN 'Visiteurs' ?

A. Tous les services internes de l'entreprise

B. Uniquement les serveurs DNS et DHCP

C. Les serveurs de messagerie et intranet

D. Les bases de données métier

Réponse correcte : B

Votre réponse : C X Incorrect

Question 17 :

Question 17

Quelle est la structure hiérarchique des visiteurs médicaux ?

A. Visiteur → Délégué régional → Responsable de secteur

B. Visiteur → Responsable de secteur → Délégué régional

C. Visiteur → Directeur commercial → DSI

D. Visiteur → Service RH → Direction

Réponse correcte : A

Votre réponse : A ✓ Correct

Question 18 :

Question 18

Quelle technologie est de plus en plus utilisée pour les serveurs chez GSB ?

A. Les mainframes

B. La virtualisation

C. Les containers Docker

D. Le cloud hybride

Réponse correcte : B

Votre réponse : B ✓ Correct

Question 19 :

Question 19

Quel service souhaite avoir des remontées d'information plus directes des visiteurs ?

A. Le service Rédaction

B. Le service Comptabilité

C. Le service Juridique

D. Le service Communication

Réponse correcte : A

Votre réponse : A ✓ Correct

Question 20 :

Question 20

Quelle est la principale raison du turn-over important des visiteurs ?

A. Les salaires trop bas

B. Les fusions récentes et réorganisations

C. Le manque de formation

D. Les conditions de travail difficiles

Réponse correcte : B

Votre réponse : B ✓ Correct

Conclusion :

Au cours du TP, j'ai trouvé cela intéressant car elle a permis de m'élargir les connaissances à mener une recherche, d'améliorer ma capacité à analyser des documents et à la compréhension.

J'ai trouvé ce TP très enrichissant aux connaissances.